Informatie Theorie (INT)

Informatietheorie en coderingstheorie

Gebaseerd op de kansrekening.

Ontstaan: 1948 Claude E. Shannon
"The Mathematical Theory Of Communication"
BSTJ Jul/oct. 48

Voorlopers: Hartley
Nyquist (1928)

Coderingstheorie: Hamming (1950)

Het begrip informatie:

In deze theorie werken we met een minimaal informatiebegrip; we houden namelijk alleen rekening met de theoretisch mogelijke opeenvolgingen van symbolen

1) Symbolen en signalen (syntaxis)

We houden geen rekening met:

2) Betekenissen (meaning, semantiek)

Elke informatiebron bezit redundantie (overvloedigheid)

Twee bronnen van redundantie:

1) De verschillende symbolen hebben verschillende kansen van optreden. Redundantie wordt minimaal bij symmetrisch kansveld.

2) De kansen van optreden van de symbolen worden bepaald door de voorgeschiedenis. van de bron.

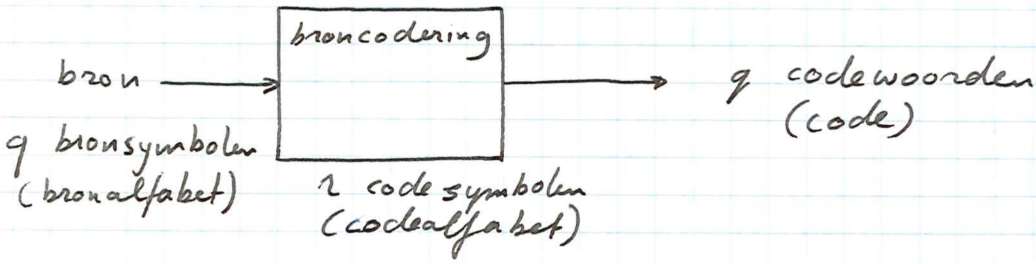
Eerste geval: bron zonder geheugen.
Tweede geval: bron met geheugen.

We willen nu met een coderingsproces, broncodering genaamd, de redundantie verwijderen. (1e theorema van Shannon).
Na broncodering volgt i.h.a een tweede coderingsslag, namelijk kanaalcodering. Hierbij wordt gest tweede redundantie toegevoegd ter bescherming tegen transmissiefouten (2e theorema van Shannon)

Inhoud van het Vak:

1) Broncodering van bronnen zonder geheugen
2) Begrip informatie; entropie
3) 1e theorema van Shannon
4) Broncodering bronnen met geheugen
5) Het gestoorde kanaal / capaciteits formule
6) 2e theorema van Shannon
7) Kanaalcodering

Broncodering voor bronnen zonder geheugen



uitgangspunten :
1) codewoorden hebben verschillende lengten
(lengte = aantal codesymbolen per woord)
2) codesymbolen hebben dezelfde lengte
(lengte = tijdsduur)

Doel van codering :

Bij gegeven q en r moet gemiddelde codewoordlengte geminimaliseerd worden.

bewenste eigenschappen

1) Ondubbelzinnig decodeerbaar

2) Code moet direct decodeerbaar zijn

Interpretatie van een codewoord is niet afhankelijk van nog te ontvangen codewoorden

Vb: $q = 4$; $r = 2$

s_1	0	← moet wachten tot er een 1 of 0 gevolgd is voordat s_1 geïnterpreteerd kan worden
s_2	01	
s_3	011	Niet DD
s_4	0111	

s_1 0
s_2 01
s_3 011
s_4 111

Niet DD
→ ontvangen : 0111111111111111
afwachten tot er een <u>0</u> komt en dan terugwerken!

s_1 0 0
s_2 0 1
s_3 1 0
s_4 1 1

Wel DD: alle codewoorden hebben lengte ≥
Blokkode

s_1 0
s_2 1 0
s_3 1 1 0
s_4 1 1 1 ~~0~~

Deze code heet een <u>komma-code</u> en is <u>redundant</u> (zie blauw kruisje)
DD op basis van komma + max. lengte

$q = 6$; $r = 2$; blokkode

s_1 0 0 0
s_2 0 0 1
s_3 0 1 0
s_4 0 1 1
s_5 1 0 ~~X~~
s_6 1 1 ~~X~~

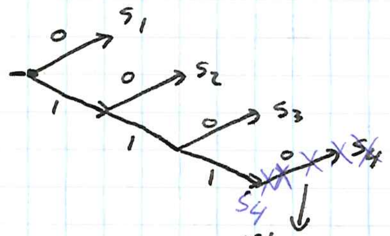
→ Als $q \neq r^n$: verkorte blokcode

zijn overbodig

<u>Voorwaarde</u> : geen codewoord begint met een ander kodewoord

We kunnen dan een decodeerboom tekenen

bv: komma-code



dit is een dode tak

en dode takken gooien we weg

Wat is nu beter, de komma- of de broncode?

Dit is afhankelijk van de kansverdeling van de bron.

Gemiddelde codewoordlengte = verwachting van codewoordlengte

$S_1 \to P_1$ verwachting $= E\{\underline{l}\} = \sum_{i=1}^{q} p_i s_i$

$S_2 \to P_2$

$S_3 \to P_3$

$S_4 \to P_4$

$\downarrow$

$\sum p = 1$

Vb: 0,2; 0,25; 0,25; 0,3;

Blok $\Rightarrow E\{\underline{b}\} \Rightarrow \underline{\underline{2}}$

komma $\Rightarrow E\{\underline{b}\} \Rightarrow = 0,3 \cdot 1 + 0,25 \cdot 2 + 0,25 \cdot 3 + 0,2 \cdot 3 = \underline{\underline{2,15}}$

Vb: 0,1; 0,15; 0,15; 0,6

komma $\Rightarrow 0,6 \cdot 1 + 0,15 \cdot 2 + 0,15 \cdot 3 + 0,1 \cdot 3 = \underline{\underline{1,65}}$

Noodzakelijke en voldoende voorwaarde voor het bestaan van de DD-code:

codewoordlengte

Ongelijkheid van Kraft: $k = \sum_{i=1}^{q} r^{-l_i} \leq 1$

Bewijs!

Stel: aantal codewoorden met $l = 1$: w_1

$(w_1 \leq r)$

we houden over $r - w_1$ symbolen voor langere codewoorden

aantal codewoorden met lengte $l = 2$: w_2

$w_2 \leq (r - w_1) \cdot r$

resteert: $(r - w_1) r - w_2$

$\Rightarrow w_3 \leq \{(r - w_1) r - w_2\} \cdot r$

$\leq r^3 - r^2 w_1 - r w_2$

resteert: $r^3 - r^2 w_1 - r w_2 - w_3$

$w_4 \leq r^4 - r^3 w_1 - r^2 w_2 - r w_3$

maximale lengte is m:

$$w_m \leq r^m - r^{(m-1)} \cdot w_1 - \cdots - r^2 w_{m-2} - r w_{m-1}$$

Delen door r^m:

$$0 \leq 1 - w_1 r^{-1} - w_2 r^{-2} - \cdots - r^{-(m-2)} w_{m-2} - r^{-(m-1)} w_{m-1} + - r^{-m} w_m$$

$\Rightarrow \sum_{j=1}^{m} w_j r^{-j} \leq 1 \Rightarrow$ Even omwerken

4

Er staat nu eigenlijk het volgende

$$\underbrace{r^{-1} + r^{-1} + \cdots r^{-1}}_{w_1} + \underbrace{r^{-2} + r^{-2} \cdots r^{-2}}_{w_2} + \cdots$$

$$\cdots + \underbrace{r^{-m} + r^{-m} + \cdots + r^{-m}}_{w_m} \leq 1$$

$$\sum_{i=1}^{m} w_i = q$$

$$\downarrow$$

$$\sum_{i=1}^{q} r^{-l_i} \leq 1$$

Opm: Kraft geeft geen voorwaarde voor niet-bestaan van niet-DD-code.

Komma-code: $2^{-1} + 2^{-2} + 2^{-3} + 2^{-3} = 1$

$+ 2^{-4} = 0{,}9 \quad < 1$

$\downarrow$

dode tak

Nu deze code

S_1	0
S_2	01
S_3	011
S_4	0111

Niet DD

$k = 2^{-1} + 2^{-2} + 2^{-3} + 2^{-4} = 0{,}9\ldots < 1$

Opgave: Bepaal het kleinste aantal codesymbolen waarmee acht bronsymbolen kunnen worden gekodeerd in 3 woorden met $l = 2$ en 5 woorden met $l = 4$ DD-coderen

Opgave : Construeer een kommacode met $q = 13$ en $r = 3$

Ontwerp van een efficiente DD-code

We schryven voor de $E\{b\} = L$

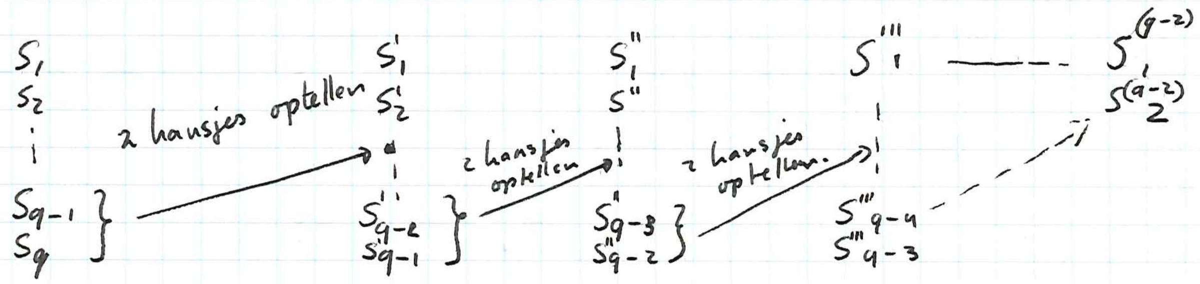
Efficientie $\eta = \frac{a}{L}$ (a later bepalen)

principe : Als $P_1 \geq P_2 \geq P_3 \geq \ldots \geq P_q$ $(\sum P_i = 1)$

dan moet $L_1 \leq L_2 \leq L_3 \ldots \leq L_q$

De Huffmancode

Eerst $r = 2$.



$(P_i \geq P_{i+1})$

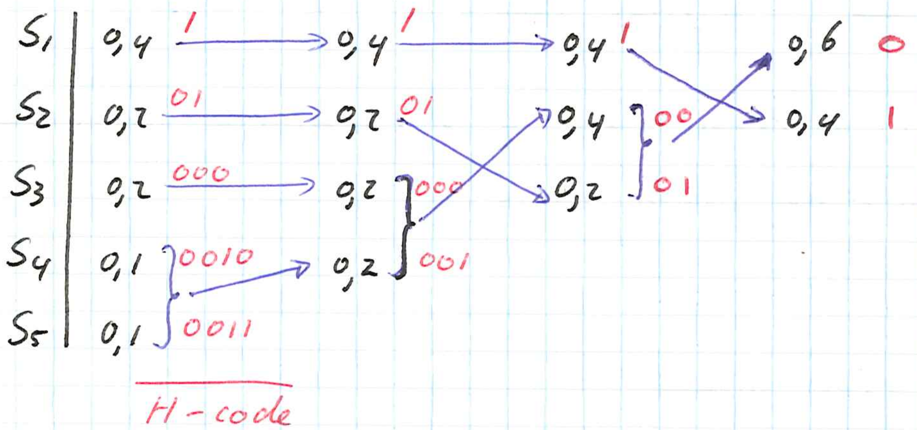
We nemen S_{q-1} en S_q samen tot 1 symbool en maken zo een denkbeeldige nieuwe bron met $q-1$ symbolen. Weer rangschikken volgens afnemende kans.

Herhaal dit proces (dus telkens: twee minst waarschynlyke symbolen onderin de lyst, dus boven in de boom, en met even lange codewoorden) tot slechts 2 symbolen overblijven.
Deze miniboom krijgt de vanzelfsprekende kode (meest efficiente) : $S_1^{(q-2)} = 0$

$S_2^{(q-2)} = 1$

Laat nu de boom weer uitlopen op dezelfde wijze waarop hij gesnoeid is, dus: voeg bij elk nieuw paar takken een 0 en een 1 toe.

VB: $q = 5$ $P = \{0{,}4;\ 0{,}2;\ 0{,}2;\ 0{,}1;\ 0{,}1\}$



Opm 1: bij elk paar nieuwe takken mag de volgorde van 0 en 1 willekeurig gekozen worden. Hierdoor ontstaat geen andere fundamentele code

Opm 2: indien, zoals hier, de som van 2 kansen een andere bestaande kanswaarde geeft, dan zijn ook alternatieve schema's mogelijk. Deze kunnen ander H-code's geven

Opgave: stel voor dit voorbeeld de 5 andere H-code schema's op

$$L = 0{,}4 + 0{,}2.2 + 0{,}2.3 + 0{,}1.4 + 0{,}1.4 = 2{,}2$$

Alternatieve codes geven dezelfde L, maar een andere spreiding. Hoog wegplaatsen geeft minste spreiding (→ blokcode)

$$\sqrt{\sum_i p_i (l_i - L)^2}$$

RMS van de afwijking van de verwachting

Bij $r > 2$ geldt de redenering die tot de H-code leidde weer, m.d.v dat telkens r symbolen tegelijk ~~worden~~ worden weggesnoeid. Om een miniboom met r takken te verkrijgen moet dan:

$$\frac{q-r}{r-1} \quad \underline{\text{geheel}} \text{ zijn}$$

Is hieraan niet voldaan dan q kunstmatig vergroten met dummy-symbolen met kans $\frac{0}{\ }$.

VB: $q = 8 \quad r = 3$

$$\frac{q-r}{r-1} = 2,5 \quad \text{niet geheel}$$

maak $\frac{q-r}{r-1} = 3 \Rightarrow q$ moet $\underline{9}$ zijn

		H-code						
S_1	0,22	2	0,22	2	0,25	1	0,53	0
S_2	0,20	00	0,20	00	0,22	2	0,25	1
S_3	0,18	01	0,18	01	0,20	00	0,22	2
S_4	0,15	02	0,15	02	0,18	01		
S_5	0,10	10	0,10	10	0,15	02		
S_6	0,08	11	0,08	11				
S_7	0,05	120	0,07	12				
S_8	0,02	121						
S_9 (dummy)	0,00	122	← Deze weg					

De Huffman-code is de meest efficiente codering (DD) van geheugenvrije bronnen.

Bewijs (voor $r = 2$ → binair):

Stel er is een rivaalcode waarvoor geldt:

$$L_{RIVAAL} < L_{HUFFMAN}.$$

Nu beide bomen insnoeien:

Bij Huffman: Reductie per snoeislag bepalen:

Bijdrage aan L voor snoeien:

$\Rightarrow P_q \cdot l_q + P_{q-1} \cdot l_{q-1}$

$\Rightarrow P_q \cdot l_q + P_{q-1} \cdot l_q$

$\Rightarrow (P_q + P_{q-1}) \cdot l_{q-1}$

Na snoeien:

$$(P_q + P_{q-1}) \cdot (l_{q-1} - 1)$$

De reductie is: $P_q + P_{q-1}$ (onafhankelijk van de boomstructuur)

Dit geldt ook in elke fase van het snoeiproces voor de rivaalcode

H: $L = 1$ → R: $L < 1$ → miniboom bestaat niet.

Verdere vergroting van de efficientie is mogelijk door hogere uitbreidingen van het bronalfabet te coderen

De n^e uitbreiding van S is S^n, de verzameling van alle combinaties van n symbolen uit S

opgave:

$q = 13 \qquad r = 3 \qquad C = \{0, 1, 2\}$

0
10
20
110
120
210
220 ← dood hout
1110
1120
1210
1220
2110
2120
13 ———
2210
2220

Vb: $S = \{s_1, s_2\}$ met $P\{\frac{2}{3}, \frac{1}{3}\}$ en $C = \{0, 1\}$

1e uitbreiding :

S'	Codew
s_1	0
s_2	1

$L_1 = 1$

2e uitbreiding :

S^2	Codew
$s_1 s_1$	1
$s_1 s_2$	01
$s_2 s_1$	000
$s_2 s_2$	001

4/9	1	4/9	1	5/9	0
2/9	01	3/9	00	4/9	1
2/9	000	2/9	01		
1/9	001				

$L_2 = \frac{4}{9} + \frac{2}{9}\cdot 2 + \frac{2}{9}\cdot 3 + \frac{1}{9}\cdot 3$
$= \frac{17}{9} \approx 2$

per oorspronkelijk bronsymbool :

$L_2' = \frac{L_2}{2} = \frac{17}{18} < 1 \longrightarrow$ winst
↳ 0,9444

3e uitbreiding :

$s_1 s_1 s_1$	8 01	8 01	8 01	8 01	8 00	11 1	16 0
$s_1 s_1 s_2$	4 000	4 000	4 11	7 10	8 01	8 00	11 1
$s_1 s_2 s_1$	4 001	4 001	4 000	4 11	7 10	8 01	
$s_2 s_1 s_1$	4 100	4 100	4 001	4 000	4 11		
$s_1 s_2 s_2$	2 110	3 101	4 100	4 001			
$s_2 s_1 s_2$	2 111	2 110	3 101				
$s_2 s_2 s_1$	2 010	2 111					
$s_2 s_2 s_2$	1 011						

$L_3 = \frac{1}{27}\{8\times 2 + 4\times 3\times 3 + 2\times 3\times 2 + 2\times 4 + 1\times 4\} = \frac{76}{27}$

$$L_3' = \frac{L_3}{3} = \frac{76}{81} = 0{,}9382$$

n	L_n'
1	1,000
2	0,944
3	0,938
4	0,930
5	0,923

Limiet : 0,91830 (entropie)
(later aantonen)

Limiet is afhankelijk van $\mathcal{F}$ en R

waar gaat dit heen!

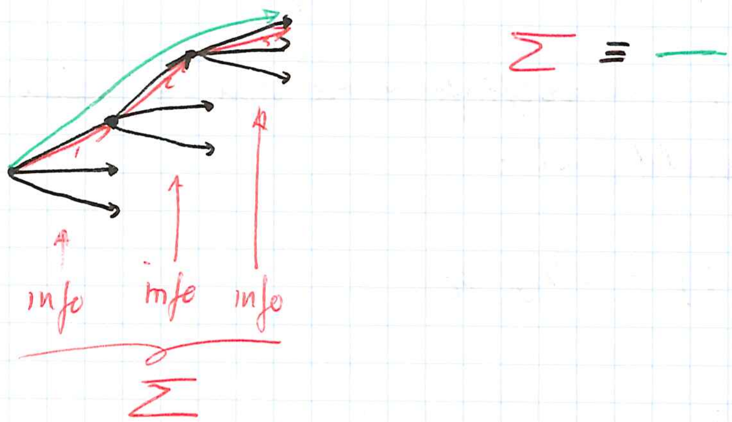
<u>Het begrip informatie</u>

Informatie komt vrij bij het wegnemen van <u>onzekerheid</u>.
<u>Ook</u>: Informatie als hoeveelheid verrassing

Hieruit volgt :

1) hoeveelheid info is monotoon stijgende functie van aantal keuzemogelijkheden .(d.i. q)

Hierbij is voorlopig een symmetrisch kansveld verondersteld



Voorwaarde 2: Bij het maken van een aantal keuzen achter een moet de hoeveelheid info verkregen worden door info, hoewel totaal aantal eindkeuzen verkregen wordt door vermenigvuldiging.

$$J(n \cdot m \cdot k) = J(n) + J(m) + J(k)$$

Hieraan voldoet alleen : $I(x) = c \ln x$

Keuze 1:

1) $c = 1 \rightarrow I(x) = \ln x \longrightarrow$ <u>Nat</u>

2) $c = {}^{2}\log e \rightarrow I(x) = {}^{2}\log e \cdot {}^{e}\log x \longrightarrow {}^{2}\log x \longrightarrow$ <u>bit</u>

3) $c = {}^{10}\log e \rightarrow I(x) = {}^{10}\log x \rightarrow$ <u>Hartley</u>

keuze uit twee mogelykheden $P = \{\frac{1}{2}, \frac{1}{2}\}$

$$I = {}^{2}\log 2 = 1 \text{ bit}$$

keuze uit drie mogelijkheden : $P = \{\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\}$

$$I = {}^{2}\log 3 \simeq 1{,}58 \text{ bit}$$

Nu een <u>niet-symmetrisch</u> kansveld:

In het voorgaande was:

$$I = {}^{2}\log n = {}^{2}\log \frac{1}{p}$$

met $p = p_1 = p_2 \quad p_3 = p_q$

Voeren we nu in: de zelfinformatie van de gebeurtenis uit een niet sym. kansveld, als:

$$I(\text{geb. } i) = -{}^{2}\log p_i$$

VB: $q = 3 \quad P = \{0{,}80 \,;\, 0{,}15 \,;\, 0{,}05\}$

$$J_{s1} = -{}^{2}\log 0{,}8 = 0{,}32$$

$$J_{s2} = -{}^{2}\log 0{,}15 = 2{,}74$$

$$J_{s3} = -{}^{2}\log 0{,}05 = 4{,}32$$

We zijn geïnteresseerd in de gemiddelde hoeveelheid info bij deze bron.

$$E\{I\} = 0{,}8 \cdot 0{,}32 + 0{,}15 \cdot 2{,}74 + 0{,}05 \cdot 4{,}32$$
$$= 0{,}88$$

dus: <u>redundantie</u>.

Gemiddelde hoeveelheid info/sym: $\sum_{i=1}^{q} p_i \cdot {}^2\log \frac{1}{p_i}$

Wordt de <u>entropie</u> van de van de bron genoemd $[=H(S)]$

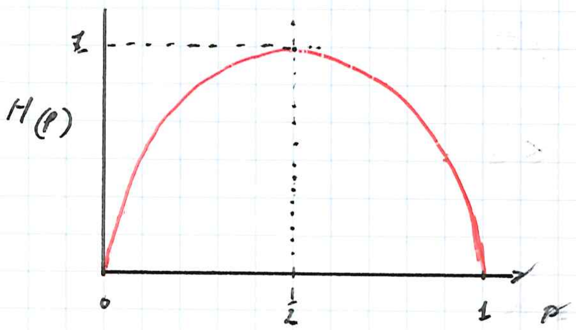
<u>Binaire bron</u>:

$$H(S) \;\; -p\,{}^2\log p - (1-p)\,{}^2\log(1-p)$$

$$\frac{d\,H(S)}{dp} = -{}^2\log p \cancel{- p \cdot {}^2\log e \cdot \frac{1}{p}} + {}^2\log(1-p) \cancel{-(1-p)\,{}^2\log e \,\frac{1}{1-p} \cdot -1}$$

$$= {}^2\log \frac{1-p}{p} = 0$$

$$\frac{1-p}{p} = 1 \implies \text{dus } \underline{\underline{p = \tfrac{1}{2}}}$$



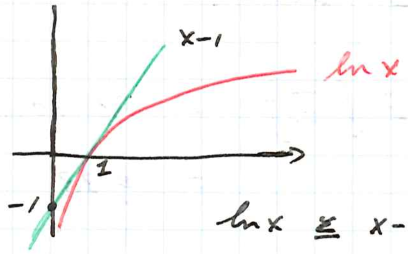
<u>Nu $q > 2$</u>:

$$H(S) - {}^2\log q = -\sum_{i=1}^{q} p_i\,{}^2\log p_i - {}^2\log q \cdot \overbrace{\sum_{i=1}^{q} p_i}^{=1}$$

$$= \quad '' \quad - \sum_{i=1}^{q} p_i \log q$$

$$= - \sum_{i=1}^{q} p_i \, {}^2\log p_i q = \sum_{i=1}^{q} p_i \, {}^2\log \frac{1}{p_i q}$$

Opm: voor $\ln x$ geldt:



$\ln x \leq x-1$

dus:

$$H(S) - {}^2\log q \leq + \sum_{i=1}^{q} p_i \, {}^2\log e \cdot \left(\frac{1}{p_i q} - 1\right)$$

$$\leq + \sum_{i=1}^{q} {}^2\log e \cdot \left(\frac{1}{q} - p_i\right)$$

$$\leq {}^2\log e \cdot \left\{ \underbrace{\sum_{i=1}^{q} \frac{1}{q}} - \underbrace{\sum_{i=1}^{q} p_i} \right\}$$

$$\leq {}^2\log e \left\{ 1 - 1 \right\} = 0$$

"=" teken als $\frac{1}{p_i q} = 1$

voor alle p_i : $p_i = \frac{1}{q}$

<u>Verband tussen L en H(S):</u>

Gaan we uit van Kraft:

$$k = \sum_{i=1}^{q} 2^{-l_i} \leq 1$$

$$1 = \underbrace{\sum_{i=1}^{q} \frac{2^{-l_i}}{k}}_{\sum_{i=1}^{q} Q_i} \leq \frac{1}{k}$$

Opm: Indien $\sum_{i=1}^{q} x_i = 1$ en $\sum_{i=1}^{q} y_i = 1$ dan geldt

$$\sum_{i=1}^{q} x_i \, {}^2\log \frac{y_i}{x_i} \leq 0$$

Eenvoudig na te gaan m.b.v. de ongelijkheid $\ln x < x-1$

Nu geldt: $\sum_{i=1}^{q} Q_i = 1$ en $\sum_{i=1}^{q} p_i = 1$

dus: $$\sum_{i=1}^{q} p_i \, {}^2\log \frac{Q_i}{p_i} \le 0$$

$$\sum_{i=1}^{q} p_i \log \frac{1}{p_i} \le -\sum_{i=1}^{q} p_i \log Q_i$$

$$H(S) \le -\sum_{i=1}^{q} p_i \log \frac{r^{-l_i}}{k}$$

$$\le +\underbrace{\sum_{i=1}^{q} p_i l_i}_{L} \log r + \log k \underbrace{\sum_{i=1}^{q} p_i}_{1}$$

$$\le \log r \cdot L + \log k \cdot 1$$

$k \le 1 \rightarrow \log k \le 0$

Zeker geldt: $H(S) \le \log r \cdot L$

Neem eerst even de binaire codering:

$$H(S) \le L$$

infobit/sy $\le$ bin. digit/sy

Een Binary digit kan niet meer dan 1 info bit bevatten. (Uiteraard wel)

$r > 2$

$$\frac{H(S)}{\log r} \le L \rightarrow \frac{-\sum_{i=1}^{q} p_i \, {}^2\log p_i}{\log r} \le L$$

$$\frac{\log p_i}{\log r} = {}^r\log p_i \rightarrow -\sum_{i=1}^{q} p_i \, {}^r\log p_i \le L$$

$$H_r(S) \le L$$

entropie op radix-basis

! **Bewijs: 1e Theorema van Shannon**

We introduceren de broncodering volgens Shannon:

Recept: $\underline{{}^{r}\log \frac{1}{p_i} \leq l_i < {}^{r}\log \frac{1}{p_i} + 1}$

Toetsen aan Kraft:

$${}^{r}\log \frac{1}{p_i} \leq {}^{r}\log r^{l_i} < {}^{r}\log \frac{1}{p_i} + {}^{r}\log r$$

$$\frac{1}{p_i} \leq r^{l_i} < \frac{r}{p_i}$$

$$p_i \geq r^{-l_i} > \frac{p_i}{r}$$

$$\underbrace{\sum_{i=1}^{q} p_i}_{1} \geq \sum_{i=1}^{q} r^{-l_i} > \underbrace{\sum_{i=1}^{q} \frac{p_i}{r}}_{\frac{1}{r}}$$

$$\underbrace{1 \geq \sum_{i=1}^{q} r^{-l_i} > \frac{1}{r}}_{\text{Kraft !}}$$

<u>Kraft</u> ! → gezond recept

nu bewijs 1e theorema

uit recept volgt:

$$\sum_i p_i \, {}^{r}\log \frac{1}{p_i} \leq \sum_i p_i l_i < \sum_i p_i + \sum_i p_i \, {}^{r}\log \frac{1}{p_i}$$

$$H_r(S) \leq L < 1 + H_r(S)$$

***

Hogere uitbreidingen $H(S^2) = ?\ H(S)$.

↳ $H(S^n) = n\,H(S)$

(n aantal bronsymbolen $s_1\, s_2\, s_3\, s_4\, ---$)

***

n^e uitbreiding met Shannon

$$H_2(S^n) \leq L_n < 1 + H_2(S^n)$$

$$n\,H_2(S) \leq L_n < 1 + n\,H_2(S)$$

$$H_2(S) \leq \frac{L_n}{n} < \frac{1}{n} + H_2(S)$$

$$H_2(S) \leq L'_n < \frac{1}{n} + H_2(S)$$

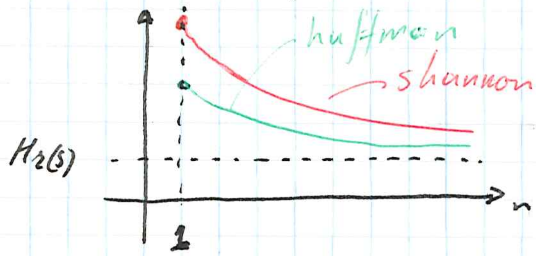
nu : $n \to \infty$

$$\boxed{\lim_{n\to\infty} L'_n = H_2(S)}$$

1e Theorema van Shannon

In woorden :

Door steeds hogere uitbreidingen van de bron te coderen kan L'_n de entropie $H_2(S)$ willekeurig dicht benaderen, d.w.z. kan de redundantie willekeurig klein gemaakt worden.

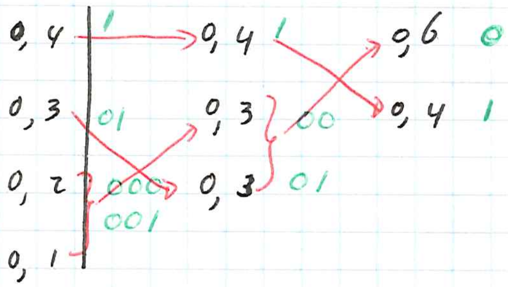


Huffman is altijd beter dan Shannon

Voorbeeld :

$Q = 4 \qquad P\{0,4 ; 0,3 ; 0,2 ; 0,1\} \qquad r = 2$

Huff:



$L_{huff} = 0,4.1 + 0,3.2 + 0,2.3 + 0,1.3$

$= \underline{\underline{1,9}}$

Shannon :

$^2\log \frac{1}{0,4} \leq l_1 < 1 + {}^2\log \frac{1}{0,4}$

$1,.. \leq l_1 < 2,... \longrightarrow l_1 = 2$

$- -$

$1, ... \leq l_2 < 2, ... \longrightarrow l_2 = 2$

$2, ... \leq l_3 < 3, .. \longrightarrow l_3 = 3$

$3 ... \leq l_4 < 4, ... \longrightarrow l_4 = 4$

$L_{sh} = 0,4 . 2 + 0,3.2 + 0,2 . 3 + 0,1 . 4$

$= \underline{\underline{2,4}}$

Vb2 : $\quad Q = 2 \qquad P = \left(\frac{2}{3}, \frac{1}{3}\right) \qquad r = 2$

n	L'_{h}	L'_{s}
1	1,000	1,333
2	0,944	1,333
3	0,938	1,000
4	0,938	1,083
5	0,923	0,933
6		1,000

Entropie $H(S) =$

$= \frac{2}{3} \, {}^2\log \frac{3}{2} + \frac{1}{3} \, {}^2\log 3$

$= \underline{\underline{0,918}}$

$$\eta_{code} = \frac{a}{L} \quad \text{wordt dus :}$$

$$\boxed{\eta_{code} = \frac{H_r(S)}{L}}$$

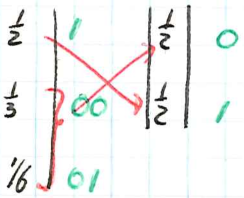
Vb: $\quad Q = 3 \quad P = \left(\frac{1}{2}, \frac{1}{3}, \frac{1}{6}\right) \quad r = 2$

$$H(S) = \frac{1}{2}\,{}^2\log 2 + \frac{1}{3}\,{}^2\log 3 + \frac{1}{6}\,{}^2\log 6 = 1{,}45914 \ldots \text{ bit/sym}$$

$$\eta_{code} = \frac{H_q(S)}{L} = \frac{H(S)}{{}^2\log q \cdot L} = \frac{1{,}45914}{\log 3}$$

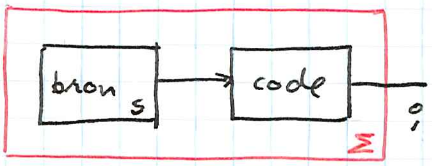
$$= 0{,}92062$$

Huffman



$$L = \frac{1}{2}\cdot 1 + \frac{1}{3}\cdot 2 + \frac{1}{6}\cdot 2 = 1{,}5$$

$$\eta_{na\ codering} = \frac{1{,}45914}{1{,}5} = 0{,}97277$$



Een externe waarnemer bepaald de kans op een 0 en een 1 van bron Σ

een modelboodschap opstellen: (dat doen wy)

| 1 | 1 | 1 | 0 0 | 0 0 | 0 1 |

aantal eenen = 4 , nullen = 5

$$\left.\begin{array}{l}\text{eenen} = 4\\ \text{nullen} = 5\end{array}\right\} \; p\{1\} = \frac{4}{9} \rightarrow p\{0\} = \frac{5}{9}$$

$$H(\Sigma) = \frac{4}{9} \log \frac{9}{4} + \frac{5}{9} \log \frac{9}{5} = 0{,}99108$$

Wat is nu entropie per symbool van S:

$$\underbrace{L \cdot H(\Sigma)}_{H(S)} = 1{,}5 \cdot 0{,}99108$$

$$H(S) = 1{,}4866$$

Maar bekend: $H(S) = \underline{\underline{1{,}45914}}$. ??

Bron Σ heeft geheugen!

Het 1e antwoord is onjuist omdat bron Σ geheugen heeft (interne structuur die de samenhangen van opeenvolgende nullen en enen min of meer vastlegt), en formule voor H(S) ontworpen voor de geheugenvrije bron.

Een Bron Met Geheugen

Z: zonnig
B: bewolkt, droog
N: neerslag

Vandaag: Z — kans op Z morgen $P\{Z/Z\}$
" " B "
" " N "

Vandaag: B — kans op Z morgen $P\{Z/B\}$
" " B "
" " N "

Vandaag: N — kans op Z morgen $P\{Z/N\}$
" " B "
" " N "

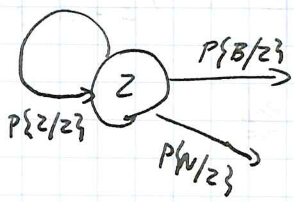
In dit voorbeeld nemen we aan dat alleen de vorige dag beïnvloed ; geheugen is 1 waarneming diep. We spreken dan van een eerste orde Markov-process

In plaats van "gewone" kansen spelen conditionele kansen een rol:

$$p\{Z/Z\} + p\{B/Z\} + p\{N/Z\} = 1^{*)}$$

*) Σ uitgaande stromen $= 1$

Vandaag	Bewolkt morgen
Z	$p\{B/Z\}$
B	$p\{B/B\}$
N	$p\{B/N\}$



$$p\{B_m\} = p\{Z_v\} \cdot p\{B/Z\} + p\{B_v\} \cdot p\{B/B\} + p\{N_v\} \cdot p\{B/N\}$$

m = morgen v = vandaag

$$[p\{Z_m\}, p\{B_m\}, p\{N_m\}] =$$

$$[p\{Z_v\}, p\{B_v\}, p\{N_v\}] \cdot \begin{array}{l} \underbrace{\begin{bmatrix} p\{z/z\} & p\{b/z\} & p\{N/z\} \\ p\{z/B\} & p\{b/b\} & p\{n/b\} \\ p\{z/N\} & p\{b/N\} & p\{n/n\} \end{bmatrix}} \end{array} \begin{array}{l} \to \Sigma = 1 \\ \to \Sigma = 1 \\ \to \Sigma = 1 \end{array}$$

$\boxed{p\{a/b\} =}$

kans op a als voorige waarneming b is geweest

transitie- of overgangsmatrix
Deze beschrijft het Markov-process volledig

getallen voorbeeld

$$
T = \begin{array}{c c}
\begin{matrix} z & b & n \end{matrix} & \\
\begin{pmatrix} 1/3 & 1/3 & 1/3 \\ 1/4 & 1/2 & 1/4 \\ 1/4 & 1/4 & 1/2 \end{pmatrix} & \begin{matrix} z \\ b \\ n \end{matrix}
\end{array}
$$

1^e dag : waarneming : Z $\rightarrow$ kansvector : $(1, 0, 0)$

2^e dag : $(1, 0, 0) \cdot \begin{pmatrix} 1/3 & 1/3 & 1/3 \\ 1/4 & 1/2 & 1/4 \\ 1/4 & 1/4 & 1/2 \end{pmatrix} = \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$

3^e dag : $\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right) \cdot \begin{pmatrix} 1/3 & 1/3 & 1/3 \\ 1/4 & 1/2 & 1/4 \\ 1/4 & 1/4 & 1/2 \end{pmatrix} = \left(\frac{10}{36}, \frac{13}{36}, \frac{13}{36}\right)$

etc.

Waar gaat dit heen? Is er een stationaire toestand

dus :

$$[P\{Z\}, P\{B\}, P\{N\}] = [P\{Z\}, P\{B\}, P\{N\}] \cdot T$$

Stationaire toestand ! . .

$$
\boxed{
\begin{aligned}
p\{z\} \cdot \tfrac{1}{3} + p\{b\} \cdot \tfrac{1}{4} + p\{n\} \tfrac{1}{4} &= p\{z\} \\
p\{z\} \cdot \tfrac{1}{3} + p\{b\} \cdot \tfrac{1}{2} + p\{n\} \tfrac{1}{4} &= p\{b\} \\
p\{z\} \cdot \tfrac{1}{3} + p\{b\} \cdot \tfrac{1}{4} + p\{n\} \tfrac{1}{2} &= p\{n\}
\end{aligned}
}
$$

$$
\left.
\begin{aligned}
-\tfrac{2}{3}\, p\{z\} + \tfrac{1}{4}\, p\{b\} + \tfrac{1}{4}\, p\{n\} &= 0 \\
\tfrac{1}{3}\, p\{z\} - \tfrac{1}{2}\, p\{b\} + \tfrac{1}{4}\, p\{n\} &= 0 \\
\tfrac{1}{3}\, p\{z\} + \tfrac{1}{4}\, p\{b\} \quad \tfrac{1}{2}\, p\{n\} &= 0
\end{aligned}
\right\} \text{afhankelijk stelsel}
$$

$\Sigma = 1 \rightarrow$ $p\{z\} + p\{b\} + p\{n\} = 1$

nieuw stelsel

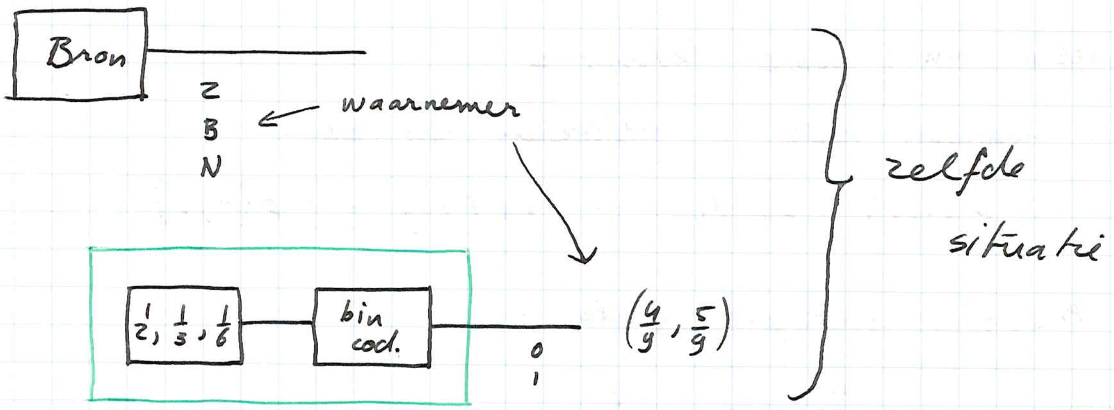
recht recht

$$\Delta = \begin{pmatrix} 1/3 & -1/2 & 1/4 \\ 1/3 & 1/4 & -1/2 \\ 1 & 1 & 1 \end{pmatrix} = \frac{11}{16}$$

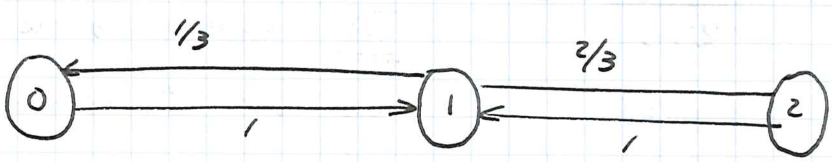
$$\Delta_z = \begin{vmatrix} 0 & -1/2 & 1/4 \\ 0 & 1/4 & -1/2 \\ 1 & 1 & 1 \end{vmatrix} = \begin{vmatrix} -\frac{1}{2} & \frac{1}{4} \\ \frac{1}{4} & -\frac{1}{2} \end{vmatrix} = \frac{3}{16}$$

$p\{z\} = \frac{3}{11}$ $\qquad$ $p\{b\} = p\{n\} = \frac{1}{2}$ van $\frac{11-3}{11}$

$= \frac{4}{11}$



convergentie treedt op bij niet-periodieke processen.



$$T = \begin{pmatrix} 0 & 1 & 0 \\ 1/3 & 0 & 2/3 \\ 0 & 1 & 0 \end{pmatrix}$$

Controleer door calculatie dat stationaire toestand niet bestaat.

Een toestandsdiagram:

bepaal alle gesloten circuits de lengten.

Als GGD van de lengten > 1 dan periodiek

Nu entropie van Markov-proces (1e orde)
(stat toestand)

neem willekeurige gebeurtenis uit het proces:

geb 1: uitkomsten $(1, ---, i, ---, n)$

geb 2: uitkomsten $(1, ---, J, -----, n)$

Neem aan: geb. 1 levert: 1

kansen voor n uitkomsten van geb. 2:

$p\{1/1\}, p\{2/1\} --- p\{J/1\} --- p\{n/1\}$

Hiermee entropie bepalen:

$$-\sum_{j=1}^{n} p\{J/1\} \, {}^2\log p\{J/1\} = H(J/1)$$

Bij uitkomst = 2 van geb. 1

$$-\sum_{j=1}^{n} p\{J/2\} \, {}^2\log p\{J/2\} = H(J/2)$$

geb. 1.		entropie bij geb 2
1	$p\{1\}$	$H\{J/1\}$
2	$p\{2\}$	$H\{J/2\}$
3	$p\{3\}$	$H\{J/3\}$
i	$p\{i\}$	$H\{J/i\}$
n	$p\{n\}$	$H\{J/n\}$

De entropie is de verwachting van de stochastische variabele $H\{J/i\}$

De entropie is dus:

$$\Rightarrow \sum_{i=1}^{n} P\{i\} \left\{ -\sum_{j=1}^{n} p\{j/i\} \, {}^{2}\log p\{j/i\} \right\}$$

$$= -\sum_{i=1}^{n} \sum_{j=1}^{n} p\{i\} \cdot p\{j/i\} \, {}^{2}\log p\{j/i\}$$

$$= H(S_m) \quad \text{of} \quad H_m(j,i)$$

Vb.:

$$\begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \end{pmatrix} \qquad \begin{array}{l} p\{Z\} = \frac{3}{11} \\ p\{N\} = p\{B\} = \frac{4}{11} \end{array}$$

1°) proces van de 0e orde met dezelfde kansen

$$H(S) = \frac{3}{11} \, {}^{2}\log \frac{11}{3} + 2 \cdot \frac{4}{11} \, {}^{2}\log \frac{11}{4} = \frac{17{,}3}{11} \quad 1{,}57$$

2°) nu eerste orde proces:

$$\left(\frac{3}{11} \cdot \frac{1}{3} \cdot {}^{2}\log 3 \right) \cdot 3 + \left[2\left(\frac{4}{11} \cdot \frac{1}{4} \log 4 \right) + \frac{4}{11} \cdot \frac{1}{2} \log 2 \right] \cdot 2$$

$$\frac{3}{11} \log 3 + \frac{8}{11} + \frac{4}{11} = \frac{16{,}75}{11} = 1{,}52$$

Na coderen:

0e orde

$\frac{4}{11}$	1	$\frac{7}{11}$	0
$\frac{4}{11}$	00	$\frac{4}{11}$	1
$\frac{3}{11}$	01		

$$L = \frac{4}{11} \cdot 1 + \frac{4}{11} \cdot 2 + \frac{3}{11} \cdot 2 = \frac{18}{11}$$

1e orde : Code laten afhangen van voorgeschiedenis

1e Vorige exp : Z

$\frac{1}{3}$	1
$\frac{1}{3}$	00
$\frac{1}{3}$	01

$L_Z = \frac{5}{3}$

2e Vorige exp : B.

$\frac{1}{2}$	1
$\frac{1}{4}$	00
$\frac{1}{4}$	01

$L_B = \frac{1}{2} \cdot \left[2 \cdot \frac{1}{4}\right] \cdot 2 = 1\frac{1}{2}$

3e Vorig exp : N

$\frac{1}{2}$	1
$\frac{1}{4}$	00
$\frac{1}{4}$	01

$L_N = 1\frac{1}{2}$

Totaal gemiddeld is de verwachting van L_i

$$\frac{3}{11} \cdot \frac{5}{3} \cdot + \frac{4}{11} \cdot \frac{6}{4} + \frac{4}{11} \cdot \frac{6}{4} = \frac{17}{11} \quad 1,55$$

$$H(S) > L_t > H(J/i)$$

Shannon : bij coderen van hogere uitbreidingen van 1e orde proces :

$$\lim_{n \to \infty} (L_t)'_n = H(J/i)$$

Opgave : Maak een code voor de 2^e uitbreiding voor deze 1^e Markov - bron

$p\{zz/z\}$, $p\{zB/z\}$ ------------- $p\{NN/z\}$ Huff 1

$p\{zz/B\}$, ------------- $p\{NN, B\}$ Huff 2

$p\{zz/N\}$, ------------- $p\{NN, N\}$ Huff 3

! $p\{\overrightarrow{a_2, b_3}^{\epsilon} / c_1\} = p\{a/c\} \cdot p\{b/a\}$

daarna is deze geheugen

1^e geheugen inhoud

Huff 1 $\rightarrow L_2 Z = \frac{19}{6} = \frac{76}{24}$

Huff 2 $\rightarrow L_2 B = \frac{73}{24}$

Huff 3 $\rightarrow L_2 N = \frac{73}{24}$

middelen $\rightarrow L_2$

$$L_2 = \underbrace{\frac{3}{11}}_{p\{z\}} \cdot \frac{19}{6} + \{\underbrace{\frac{4}{11}}_{p\{B\},\ p\{N\}} \cdot \frac{73}{24}\} \cdot 2 = \frac{3383}{1100}$$

$$L_2' = \frac{L_2}{N} = \frac{16,92}{11}$$ {vergl $\frac{17}{11}$ voor 1^e uitbr}

$\neq H\{j/i\}$

---

opgave : 2^e orde Markov proces (binair)

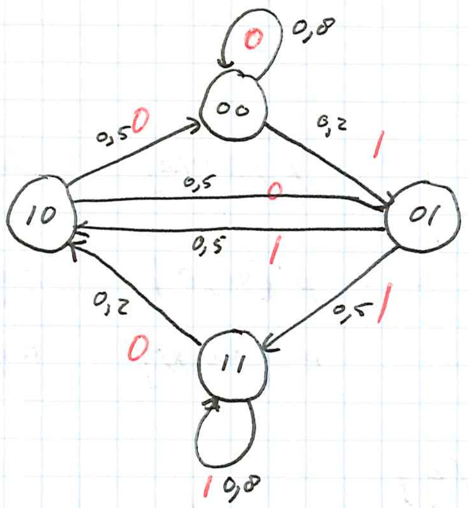
$p\{0/00\} = p\{1/11\} = \frac{8}{10}$

$p\{1/00\} = p\{0/11\} = \frac{2}{10}$

$p\{0/01\} = p\{1/10\} = p\{0/10\} = p\{1/01\} = \frac{5}{10}$.

Bepaal Entropie

$S \quad \{0,1\} \qquad p\{\overrightarrow{\underset{3}{0}/\underset{12}{00}}^{\epsilon}\} = 0{,}8$



$$p\{00\} = 0{,}8\, p\{00\} + 0{,}5\, p\{10\}$$
$$p\{01\} = 0{,}2\, p\{00\} + 0{,}5\, p\{10\}$$

$$-0{,}2\, p\{00\} + 0{,}5\, p\{10\} = 0$$
$$0{,}2\, p\{00\} - 0{,}5\, p\{10\} = 0$$
$$p\{00\} + p\{10\} = \tfrac{1}{2} \quad \leftarrow \begin{cases} p\{00\} = p\{11\} \\ p\{01\} = p\{10\} \end{cases}$$

$$1{,}4\, p\{00\} = \tfrac{1}{2}$$
$$p\{00\} = \tfrac{5}{14} = p\{11\}$$
$$p\{10\} = \tfrac{2}{14} = p\{01\}$$

Entropie : $\vec{H}\{k/ij\} = \sum\limits_i \sum\limits_j \sum\limits_k \underbrace{p\{ij\}\, p\{k/ij\}}_{\text{gewogen gemiddelde}}\, {}^2\!\log \dfrac{1}{p\{k/ij\}}$

Hier : $\left\{ \frac{5}{14} \cdot \frac{8}{10}\, {}^2\!\log \frac{10}{8} + \frac{5}{14} \cdot \frac{2}{10}\, {}^2\!\log \frac{10}{2} + \left(\frac{2}{14} \cdot \frac{1}{2}\, {}^2\!\log \frac{2}{1}\right) \cdot 2 \right\}\, 2$

$$= \frac{10}{14}\, {}^2\!\log 5 - \frac{12}{14} = 0{,}8013 \qquad (r=2)$$

$$\begin{array}{lcccc} 00 & p\{00/00\} & - & - & p\{11/00\} \\ 01 & \vdots & & & \vdots \\ 10 & \vdots & & & \vdots \\ 11 & p\{00/11\} & - & - & p\{11/11\} \end{array}$$

$$p\{\overrightarrow{\underset{34}{01}}^{\epsilon}/\overrightarrow{\underset{12}{10}}^{\epsilon}\} = p\{0/10\} \cdot p\{1/00\}$$

$$L_2 = 1{,}67 \qquad L_2' = 0{,}835$$

Note $p\{\underset{3\,4}{\overrightarrow{ab}}/\underset{1\,2}{\overrightarrow{cd}}\} = p\{a/cd\} + p\{b/da\}$

regeltje 1 2 3 4

1. cd ab $\rightarrow$ $p\{a/cd\}$ ← in geheugen!

ingeheugen! volgende is een a

daarna rode streep (venster!) opschuiven naar da

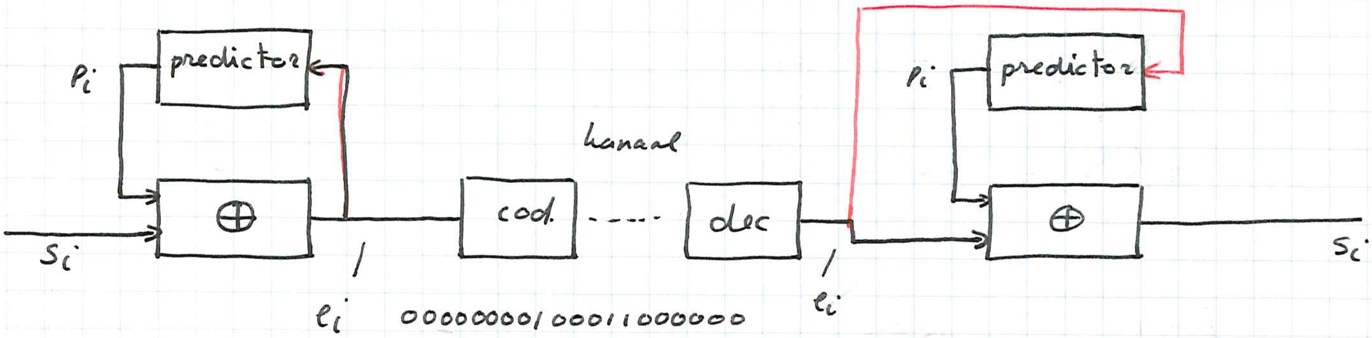
2. uit geheugen ~~c~~ d a b volgende is b $\rightarrow$ $p\{b/da\}$

in geheugen

dus $p\{ab/cd\} = \overset{1}{p\{a/cd\}} + \overset{2}{p\{b/da\}}$

Predictieve Run Encoding

Complexe binaire bronnen met veel redundantie



predictors zijn deterministisch en identiek

Een reeks nullen wordt een run genoemd

Run afgesloten met een 1

Run beschouwen als bronsymbolen

In principe ∞ veel bronsymbolen dus huffman niet te bepalen

Truuk:

Neem aan: minimaal codewoordlengte K

Runlengte	codewoordlengte
0	K
⋮	⋮
$(2^k-1)-1$	K
(2^k-1)	2K
⋮	⋮
$2(2^k-1)-1$	2K
$2(2^k-1)$	3K
⋮	⋮
$3(2^k-1)-1$	3K

$(2^k-1)\times$

$2(2^k-1)\times$

$3(2^k-1)\times$

K = 1	K = 2	K = 3
0	00	000
10	01	001
110	10	010
1110	11 00	011
11110	11 01	100
⋮	11 10	101
	11 11 00	110
	11 11 01	111 000
	11 11 10	111 001
	11 11 11 00	⋮
	⋮	

predictor beter ⟶ K groter

Kans op juiste voorspelling predictor is p

" " runlengte n is $p^n(1-p)$

$(m = 2^k - 1)$ hulpvar

$$\sum \{ \underline{\ell} \} = (1-p)k + p(p-1)k + \dots + p^{m-1}(1-p)k +$$

$$+ p^m(1-p)2k + \qquad + p^{2m-1}(1-p)2k + \dots$$

codewoordlengte

$$E\{\underline{\ell}\} = (1-p)k \cdot \{1 + p + p^2 + \dots + p^{m-1}\} +$$
$$2(1-p)kp^m \cdot \{1 + p + p^2 + \dots + p^{m-1}\} + \dots$$

eindige reeks

$$1 + p + p^2 + \dots + p^{m-1} = A$$
$$p + p^2 + \qquad + p^{m-1} + p = pA \quad -$$
$$1 - p^m = A(1-p)$$

$$E\{\underline{\ell}\} = \frac{1-p^m}{1-p}(1-p)k \cdot \{1 + 2p^m + 3p^{2m} + \dots\}$$

$$1 + p^m + p^{2m} + p^{3m} + \dots = \frac{1}{1-p^m}$$
$$p^m + p^{2m} + p^{3m} + \dots = \frac{p^m}{1-p^m}$$
$$p^{2m} + p^{3m} + \dots \quad \frac{p^{2m}}{1+p^m}$$
$$\vdots \qquad\qquad \vdots$$
$$\qquad\qquad +$$
$$1 + 2p^m + 3p^{2m} + \dots = \frac{1}{1-p^m}\{1 + p^m + p^{2m} + \dots\}$$

$$E\{\underline{\ell}\} = (1-p^m)k \frac{1}{1-p^m} \cdot \frac{1}{1-p^m}$$

$$= \frac{k}{1-p^m} = \frac{k}{1-p^{2^k-1}}$$

$k \backslash p$	0,5	0,6	0,7	0,8	0,9	0,95	0,98
ongecodeerd → 1	2	2,5	3,33	5,0	10,0	20,0	50,0
2	2,29	2,55	3,04	4,10	7,38	14,0	34,0
3			3,27	3,8	5,75	9,94	22,7
4				4,15	5,04	7,45	15,3
5					5,20	6,20	10,7
6						6,25	8,33
7						7,01	7,58
8							8,05

Bij $k=1$ datacompressie 0

$p = 0{,}8$; $k = 3$

datacompressie tot. $\frac{3{,}8}{5} = 76\%$

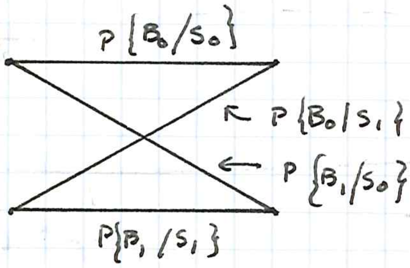
nood: minimale $E\{\ell\}$ voor bepaalde p en lopende k

Het gestoorde kanaal

Bron S — kanaal — Bestemming B

$p\{s_i\}$ $\qquad$ $p\{b_i\}$

Vb: binair kanaal $\qquad$ $p\{B_0/S_0\}$ etc zijn gegeven



$$p\{B_0\} = p\{S_0\} \cdot p\{B_0/S_0\} + p\{S_1\} \cdot p\{B_0/S_1\}$$

$$p\{B_1\} = p\{S_1\} \cdot p\{B_1/S_1\} + p\{S_0\} \cdot p\{B_1/S_0\}$$

$$P\{B\} = (p\{S\}) \cdot \begin{pmatrix} p\{B_0/S_0\} & p\{B_1/S_0\} \\ p\{B_0/S_1\} & p\{B_1/S_1\} \end{pmatrix}$$

De transmissie-matrix van het kanaal

Zend en ontvang gebeuren is te beschouwen als markov-proces met startkans $p\{S_0\}$ en $p\{S_1\}$, dat telkens na het tweede experiment wordt afgebroken en met een zelfde startkans herstart.

Stel kanaal is symmetrisch ; foutkans $\frac{1}{10}$

a) $p\{S_0\} = p\{S_1\} = \frac{1}{2} \rightarrow p\{B_0\} = p\{B_1\} = \frac{1}{2}$

a-posteriori kansen $p\{S_0/B_0\} = \frac{p\{S_0 B_0\}}{p\{B_0\}} = \frac{p\{S_0\} \cdot p\{B_0/B_0\}}{p\{B_0\}}$

(vgl : $P\{\overset{\leftrightarrow}{AB}\} = p\{A\} \cdot p\{B/A\}$)

$$p\{S_0/B_0\} = \frac{\frac{1}{2} \cdot \frac{9}{10}}{\frac{1}{2}} = \frac{9}{10}$$

b) $p\{S_0\} = \frac{19}{20} \longrightarrow p\{S_1\} = \frac{1}{20}$

$p\{B_0\} = \frac{19}{20} \cdot \frac{9}{10} + \frac{1}{20} \cdot \frac{1}{10} = \frac{172}{200}$ $\quad p\{B_1\} = \frac{1}{20} \cdot \frac{9}{10} + \frac{19}{20} \cdot \frac{1}{10} = \frac{28}{200}$

$p\{S_0/B_0\} = \dfrac{\frac{19}{20} \cdot \frac{9}{10}}{\frac{172}{200}} = \frac{171}{172}$ $\quad p\{S_1/B_0\} = \frac{1}{172}$

$p\{S_1/B_1\} = \dfrac{\frac{1}{20} \cdot \frac{9}{20}}{\frac{28}{200}} = \frac{9}{28}$ $\quad p\{S_0/B_1\} = \frac{19}{28}$

Vragen : 1 : Hoeveel info gaat er over dit kanaal ?

2 : Hoe maken we die info vrij ?

Een aantal entropien :

1) $H(S)$ = bronentropie

2) $H(B)$ = ontvangerentropie

3) $H(B/S)$, entropie van het 2^e experiment in het Markov-proses $= \sum\sum p\{S_i B_j\} \log \frac{1}{p\{B_j/S_i\}}$

gem. hoeveelheid info bij ontvanger bekend is wat er gezonden is

Ofwel : de resterende onzekerheid bij de zender na het zenden over het ontvangen symbool

irrellevante info, daarom $H\{B/S\}$: de irrelevantie

4) Nu a-posteriori : $H\{S/B\} = \sum_j \sum_i p\{S_i . B_j\} \log \frac{1}{p\{S_i/B_j\}}$

gemiddelde hoeveelheid info bij zender als bekend wat ontvangen is; ofwel : de resterende onzekerheid bij ontvanger na ontvangst over het gezonden symbool

Het betreft de relevante info die op het kanaal verloren is gegaan $H\{S/B\}$: de equivocatie

5) Gemiddelde hoeveelheid info van het gecombineerde zend-ontvang experiment.

$$H\{SB\} = \sum_i \sum_j p\{S_i B_j\} \log \frac{1}{p\{S_i B_j\}}$$

$$= - \sum_i \sum_j p\{S_i B_j\} \log p\{S_i\} +$$

$$- \sum \sum p\{S_i B_j\} \log p\{B_j / S_i\}$$

$$= - \sum_i p\{S_i\} \log p\{S_i\} \underbrace{\sum_j p\{B_j/S_i\}}_{=1} + H\{B/S\}$$

$$= H(S) + H(B/S)$$

op zelfde wijze volgt : $H\{SB\} = H\{B\} + H\{S/B\}$

Uiteraard geldt : $H\{B/S\} \leq H\{B\}$

$H\{S/B\} \leq H\{S\}$

De informatie die door het kanaal getransporteerd wordt:

Broninfo − deel dat daarvan verloren gaat

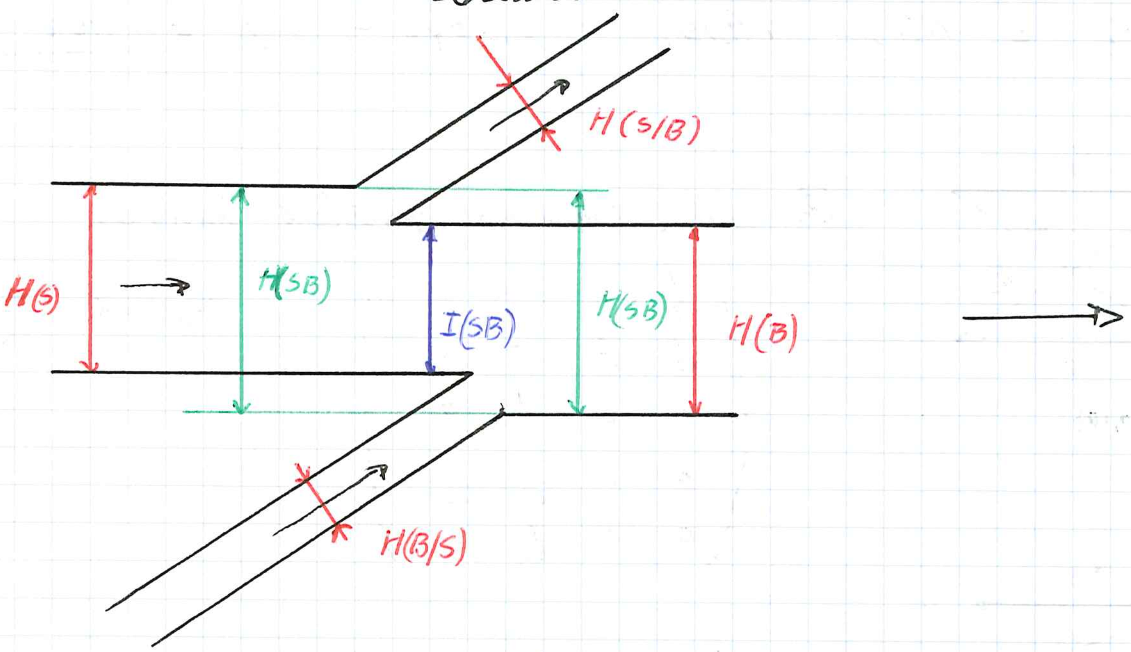
$$H(S) - H(S/B) = H(S) - [H(SB) - H(B)]$$

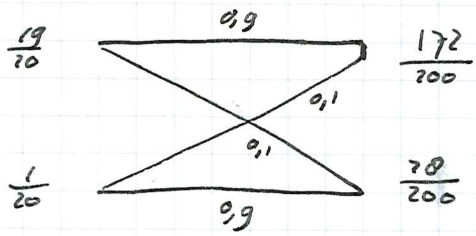
$$= H(S) - [H(S) + H(B/S) - H(B)]$$

$$= H(B) - H(B/S) = I(SB), \text{ transinfo}$$

n symbolen/sec $\rightarrow$ $n \cdot I(SB) = R(SB)$, information rate

Schema





$$p\{S_0/B_0\} = \frac{171}{172} \qquad p\{S_1/B_0\} = \frac{1}{172}$$

$$p\{S_0/B_1\} = \frac{19}{28} \qquad p\{S_1/B_1\} = \frac{9}{28}$$

$$H(S) = \frac{19}{20} \log \frac{20}{19} + \frac{1}{20} \log 20 = 0,2864$$

$$H(B) = \frac{172}{200} \log \frac{200}{172} + \frac{28}{200} \log \frac{200}{28} = 0,5842$$

$$H(B/S) = \frac{19}{20}\cdot\frac{9}{10}\log\frac{10}{9} + \frac{19}{20}\cdot\frac{1}{10}\log 10 + \frac{1}{20}\cdot\frac{1}{10}\log 10 + \frac{1}{20}\cdot\frac{9}{10}\log\frac{10}{9}$$

$$= \frac{180}{200}\log\frac{10}{9} + \frac{20}{200}\log 10 = 0{,}4690$$

$$H(S/B) = \frac{\cancel{172}}{200}\cdot\frac{171}{\cancel{172}}\log\frac{172}{171} + \frac{\cancel{172}}{200}\cdot\frac{1}{\cancel{172}}\log 172$$

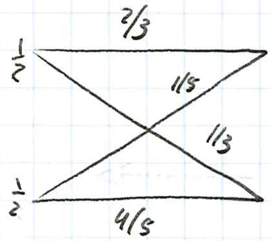
$$+ \frac{\cancel{28}}{200}\cdot\frac{19}{\cancel{28}}\log\frac{28}{19} + \frac{\cancel{28}}{200}\,\frac{9}{\cancel{28}}\log\frac{28}{9}$$

$$= 0{,}1711537391$$

$\underline{I(SB)} = H(S) - H(S/B) = 0{,}2864 - 0{,}1712 = \underline{0{,}1152}$ bit/sy

$\underline{I(SB)} = H(B) - H(B/S) = 0{,}5842 - 0{,}4690 = \underline{0{,}1152}$ bit/sy

opg/

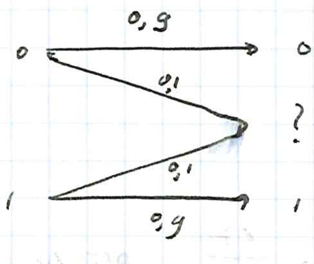
① 

~~Bhyx~~ $I(SB) = 0{,}167$

② Matrix van samengestelde kansen

$$\begin{pmatrix} \frac{1}{4} & 0 & 0 & 0 \\ \frac{1}{10} & \frac{3}{10} & 0 & 0 \\ 0 & \frac{1}{20} & \frac{1}{10} & 0 \\ 0 & 0 & \frac{1}{20} & \frac{1}{10} \\ 0 & 0 & \frac{1}{20} & 0 \end{pmatrix}$$

bepaal $I(SB)$

③ 

Binary Erasure Channel.

De kanaalcapaciteit

Def : Capaciteit is maximum van de transinformatie als daarbij alle mogelijke bronnen beschouwd worden.

Opm : Capaciteit is een kanaaleigenschap

Ongestoord kanaal : $C = \max\left(H(S) - \underbrace{H(S/B)}_{\downarrow \; =0}\right)$

$= \max H(S)$

Het uniforme kanaal

Hierbij is elke rijvector in T een permutatie van de eerste rij

$$I(SB) = H(B) - H(B/S)$$

$$= H(B) + \sum_i \sum_j p\{S_i B_j\} \log p\{B_j / S_i\}$$

$$= \quad " \quad + \underbrace{\sum_i p\{S_i\}}_{=1} \underbrace{\sum_j p\{B_j/S_i\} \log p\{B_j/S_i\}}_{\text{onafhankelijk van } i\,!}$$

$$= H(B) + \underbrace{\sum_j p\{B_j / S_1\} \log p\{B_j / S_1\}}_{\text{gegeven van het kanaal}}$$

vb $\rightarrow -H(e)$

$$\max(I(SB)) = C = \max H(B) - H(e)$$

Vb: BSC foutkans 0,1

$$\begin{pmatrix} 0{,}9 & 0{,}1 \\ 0{,}1 & 0{,}9 \end{pmatrix}$$

$$C = \underset{\max H(B)}{1} - \{0{,}9 \log \tfrac{1}{0{,}9} + 0{,}1 \log 10\}$$

$$= \underline{0{,}5310}$$

en $\begin{pmatrix} 0{,}1 & 0{,}9 \\ 0{,}1 & 0{,}9 \end{pmatrix}$ $\quad p\{B_0\} = 0{,}1$

$p\{B_1\} = 0{,}9$

$$C = \left(0{,}1 \log 10 + 0{,}9 \log \tfrac{10}{9}\right) - \left(0{,}1 \log 10 + 0{,}9 \log \tfrac{10}{9}\right)$$

---

2) $I(SB) = 1{,}256$

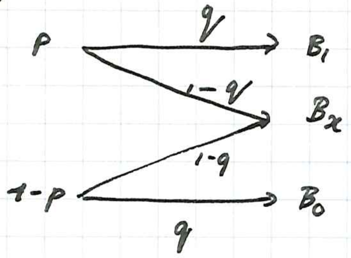
$$\begin{array}{c} p\{S_i\} \\ \frac{1}{4} \\ \frac{4}{10} \\ \frac{3}{20} \\ \frac{3}{20} \\ \frac{1}{20} \\ \\ \end{array} \begin{array}{c} \\ \leftarrow \\ \leftarrow \\ \leftarrow \\ \leftarrow \\ \leftarrow \\ \\ \end{array} \begin{array}{c} \begin{pmatrix} \frac{1}{4} & 0 & 0 & 0 \\ \frac{1}{10} & \frac{3}{10} & 0 & \\ 0 & \frac{1}{20} & \frac{1}{10} & 0 \\ 0 & 0 & \frac{1}{20} & \frac{1}{10} \\ 0 & 0 & \frac{1}{20} & 0 \end{pmatrix} \\ \begin{array}{llll} \frac{7}{20} & & & \\ p\{B_0\} & & & \end{array} \end{array} = \begin{pmatrix} p\{S_0 B_0\} & p\{S_0 B_1\} & p\{S_0 B_2\} & \cdots \\ \vdots & \vdots & \vdots & \\ p\{S_4 B_0\} & \cdots & \cdots & \cdots \end{pmatrix}$$

$$\sum_j p\{S_0 B_j\} = p\{S_0\}$$

$$\sum_i p\{S_i B_0\} = p\{B_0\}$$

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

3)



$p\{S_0/B_0\} = 1$

$p\{S_1/B_1\} = 1$

$p\{S_0/B_x\} = p$

$p\{S_1/B_x\} = 1-p$

$p\{B_0\} = pq$

$p\{B_x\} = 1-q$

$p\{B_1\} = (1-p)q$

$$I(SB) = H(S) - H(S/B)$$

$$= H(S) + [\cancel{pq \cdot 1\log 1} + (1-q)\cdot p\log p + (1-q)(1-p)\log(1-p) + \cancel{(1-p)\cdot q \cdot 1\log 1}]$$

$$= H(S) + \underbrace{\left[(1-q)\,\{p\log p + (1-p)\log(1-p)\}\right]}_{-H(S)}$$

$$= q \cdot H(S)$$

max : $C = q$

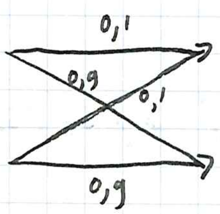
Uniform kanaal

$$I(SB) = H(B) - H(B/S) = H(B) - H(B/s_0)$$

allen gelijk

$H(C)$

$$\max[I(SB)] = \max[H(B)] - H(C)$$



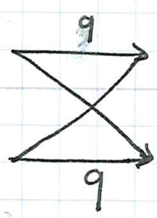
$p\{B_0\} = 0{,}1$

$p\{B_1\} = 0{,}9$

$C = (- - - -) + (\text{idem}) = 0$

Dus bij een bin. sym. channel

$$C = 1 + q\log q + (1-q)\log(1-q)$$

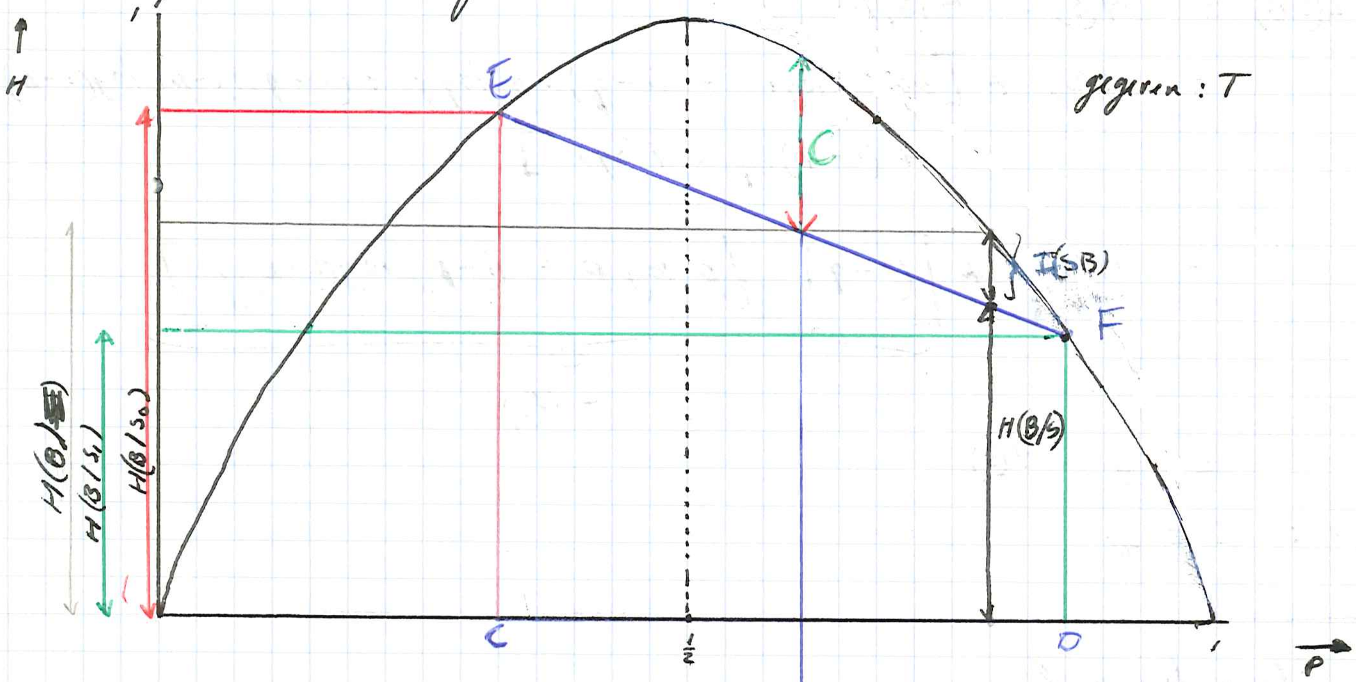


$q = 0{,}9 \qquad c = 1 + 0{,}1 \log 0{,}1 + 0{,}9 \log 0{,}9 = 0{,}531$

Vgl : BEC $\qquad C = 0{,}9$

$$\begin{pmatrix} q & 1-q & 0 \\ 0 & 1-q & q \end{pmatrix}$$

grafische bepaling van C van binair kanaal :



In tekenen $p\{B_0/S_0\}$ $\qquad p\{B_1/S_0\}$ $\qquad$ bijbehorende entropie $H(B/S_0)$

$p\{B_0/S_0\}$ $\qquad p\{B_0/S_1\}$

Intekenen $p\{B_0/S_1\}$ $\qquad p\{B_1/S_1\}$ $\qquad H(B/S_1)$

Ergens op EF ligt een punt G met entropiewaarde $H(B/S)$

$p\{B_0\} = p\{S_0\}\, p\{B_0/S_0\} + p\{S_1\}\, p\{B_0/S_1\}$

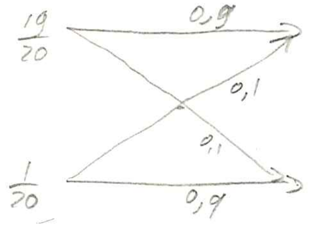
dus ergens op het interv. CD

merk op : dezelfde weegfactor als bij $H(B/S)$

$p\{B_0\}$

gewenste $P\{B_0\}$

Bronkansen zijn nu te berekenen



$$p\{B_0\} = p\{S_0\} \cdots = \frac{19}{20}\cdot 0{,}9 + \frac{1}{20}\cdot 0{,}1 = \frac{172}{200}$$

$$p\{B_1\} = p\{S_0\} \cdots = \frac{1}{20}\cdot 0{,}9 + \frac{19}{20}\, 0{,}1 = \frac{28}{200}$$

$$p\{S_0/B_0\} = \frac{p\{S_0\}}{p\{B_0\}} \cdot p\{B_0/S_0\} = \left(\frac{19}{20} \Big/ \frac{172}{200}\right) \times \frac{9}{10} = \frac{190}{172}\cdot\frac{9}{10} = \frac{171}{172}.$$

$$p\{S_1/B_0\} = \frac{p\{S_1\}}{p\{B_0\}} \cdot p\{B_0/S_1\} = \left(\frac{1}{20} \Big/ \frac{172}{200}\right) \times \frac{1}{10} = \frac{1}{172}$$

$$p\{S_0/B_1\} = \frac{p\{S_0\}}{p\{B_1\}} \cdot p\{B_1/S_0\} = \left(\frac{19}{20} \Big/ \frac{28}{200}\right) \times \frac{1}{10} = \frac{19}{28}$$

$$p\{S_1/B_1\} = \frac{p\{S_1\}}{p\{B_1\}} \cdot p\{B_1/S_1\} = \left(\frac{1}{20} \Big/ \frac{28}{200}\right) \times \frac{9}{10} = \frac{9}{28}$$

$$H(S) = \frac{19}{20}\log\frac{20}{19} + \frac{1}{20}\log 20 = 0{,}2864$$

$$H(B) = \frac{172}{200}\log\frac{200}{172} + \frac{28}{200}\log\frac{200}{28} = 0{,}5842$$

$$p\{S_0 B_0\} = p\{S_0/B_0\}\ p\{B_0\} = \qquad p\{S_0 B_1\} = p\{S_0/B_1\}\cdot p\{B_1\} =$$

$$p\{S_1 B_0\} = p\{S_1/B_0\}\ p\{B_0\} = \qquad p\{S_1 B_1\} = p\{S_1/B_1\}\cdot p\{B_1\} =$$

$$p\{S_0 B_0\} = \frac{171}{172}\cdot\frac{172}{200} = \frac{171}{200} \qquad p\{S_0 B_1\} = \frac{19}{28}\cdot\frac{28}{200} = \frac{19}{200}$$

$$p\{S_1 B_0\} = \frac{1}{172}\cdot\frac{172}{200} = \frac{1}{200} \qquad p\{S_1 B_1\} = \frac{9}{28}\cdot\frac{28}{200} = \frac{9}{200}$$

$$H\{B/S\} = \frac{171}{200}\cdot\log\frac{1}{9/10} + \frac{1}{200}\log\frac{1}{1/10} + \frac{19}{200}\log\frac{1}{1/10} + \frac{9}{200}\log\frac{1}{10/9}$$

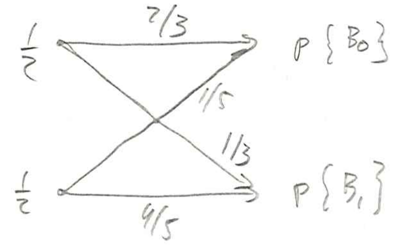
$$= \frac{180}{200}\log\frac{10}{9} + \frac{20}{200}\log 10 = 0{,}468955$$

$$H\{S/B\} = \frac{171}{200}\log\frac{172}{171} + \frac{1}{200}\log\frac{172}{1} + \frac{19}{200}\log\frac{28}{19} + \frac{9}{200}\log\frac{28}{9} = 0{,}171154$$

$$=$$

$I(SB) = H(S) - H(S/B) = 0{,}2864 - 0{,}1712 = 0{,}1152$

$H(SB) = H(B) + H(S/B) = 0{,}5842 + 0{,}1712 = 0{,}7554$



gevraagd $I(SB) =$

$$\left.\begin{aligned} p\{B_0\} &= \tfrac{1}{2}\cdot\tfrac{2}{3} + \tfrac{1}{2}\cdot\tfrac{1}{5} = \tfrac{1}{2}\cdot\left(\tfrac{2}{3}+\tfrac{1}{5}\right) = \tfrac{1}{2}\cdot\left(\tfrac{10}{15}+\tfrac{3}{15}\right) = \tfrac{13}{30}. \\ p\{B_1\} &= \tfrac{1}{2}\cdot 1/3 + \tfrac{1}{2}\cdot 4/5 = \tfrac{1}{2}\left(\tfrac{1}{3}+\tfrac{4}{5}\right) = \tfrac{1}{2}\left(\tfrac{5}{15}+\tfrac{12}{15}\right) = \tfrac{17}{30} \end{aligned}\right\} \Sigma = 1$$

$H(S) = \frac{1}{2}\log 2 + \frac{1}{2}\log 2 = 1$

$H(B) = \frac{13}{30}\log\frac{30}{13} + \frac{17}{30}\log\frac{30}{17} = 0{,}9871377742$

$p\{S_0/B_0\} = \dfrac{\frac{1}{2}}{\frac{13}{30}} \times \frac{2}{3} = \frac{10}{13}$ $\quad$ $p\{S_1/B_0\} = \dfrac{\frac{1}{2}}{\frac{13}{30}}\cdot\frac{1}{5} = \frac{3}{13}$

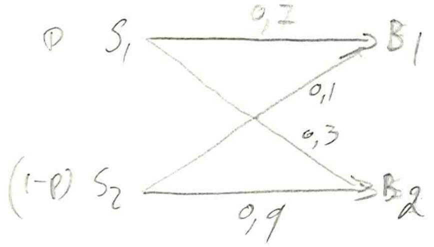
$p\{S_0/B_1\} = \dfrac{\frac{1}{2}}{\frac{17}{30}} \times \frac{1}{3} = \frac{5}{17}$ $\quad$ $p\{S_1/B_1\} = \dfrac{1/2}{\frac{17}{30}}\cdot\frac{4}{5} = \frac{12}{17}$

$p\{S_0 B_0\} = \frac{13}{30} \times \frac{10}{13} = \frac{1}{3}$ $\quad$ $p\{S_1 B_0\} = \frac{13}{30}\cdot\frac{3}{13} = \frac{1}{10}$

$p\{S_0 B_1\} = \frac{17}{30} \times \frac{5}{17} = \frac{1}{6}$ $\quad$ $p\{S_1 B_1\} = \frac{17}{30}\ \frac{12}{17}\ \frac{2}{5}$

$H\{S|B\} = \frac{1}{3}\log\frac{13}{10} + \frac{1}{10}\log\frac{13}{3} + \frac{1}{6}\log\frac{17}{5} + \frac{2}{5}\log\frac{17}{12} = 0{,}8329741901$

$I(SB) = 1 - 0{,}83297\ldots = 0{,}1670258099$



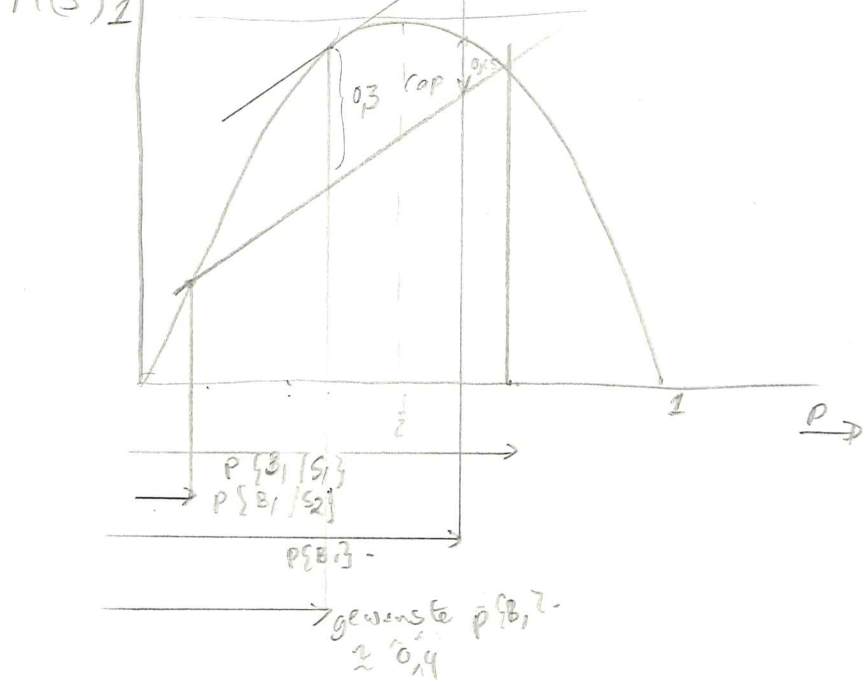
$$T = \begin{array}{ccc} B_1 & B_2 & \\ \left(\begin{matrix} 0{,}7 & 0{,}3 \\ 0{,}1 & 0{,}9 \end{matrix}\right) & & \begin{matrix} S_1 \\ S_2 \end{matrix} \end{array}$$

stel $S_1 = p$ & $S_2 = 1-p$ →

~~$p\{B_1\}$~~ = gegeven $p\{B_2\} = 0{,}4$ →

$p\{B_2\} = p \cdot 0{,}3 + (1-p)\,0{,}9 = 0{,}4$

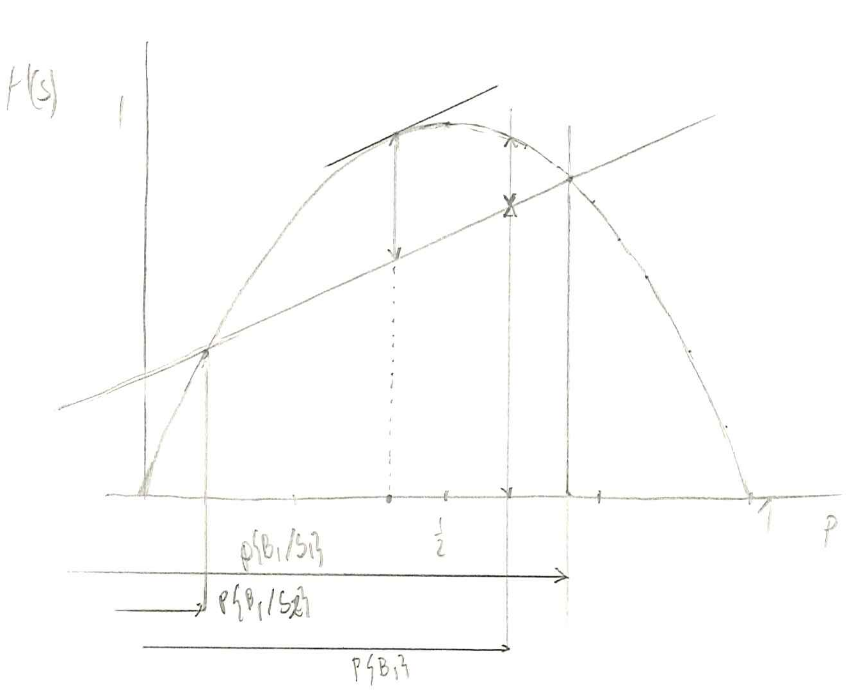
$-0{,}6p = -0{,}5 \rightarrow +6p = +5$ $\underline{p = 5/6}$



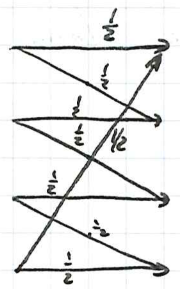
$p\{S_1\} = 5/6$

$p\{S_2\} = 1/6$

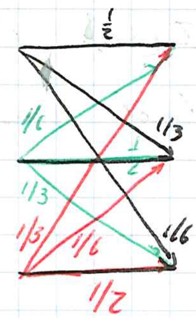
$p\{B_1\} = 5/6 \cdot 7/10 + 1/6 \cdot \frac{1}{10} = \frac{3}{5} = 0{,}6$



Opgave:



$C \overset{?}{=} 1$



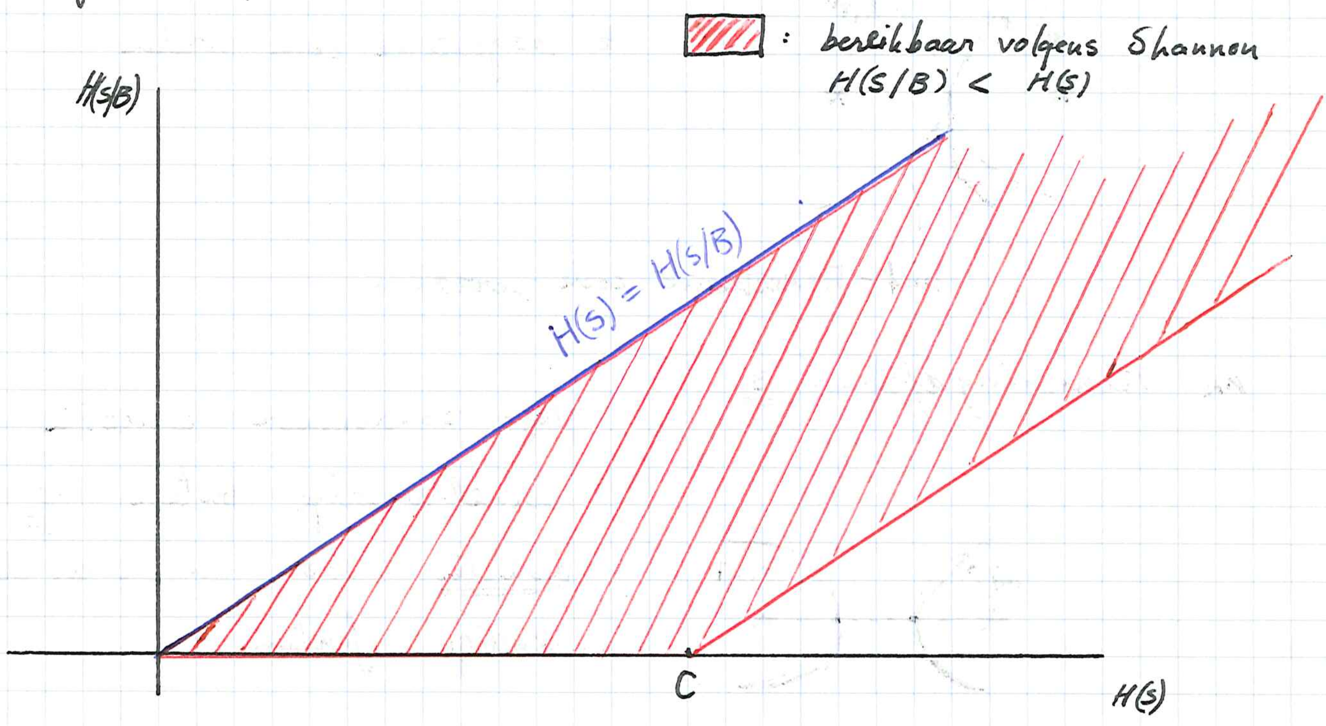
$C = 0{,}216$

Het tweede theorema van Shannon

Is op een discreet geheugenvrij kanaal met capaciteit C een discreet vrije bron aangesloten met entropie $H(S)$ en geldt $H(S) \leq C$, dan bestaat een codering ~~zodat~~ zodanig dat de informatie kan worden overgedragen met minimale foutkans (willekeurig klein) (willekeurig kleine equivocatie)

Is $H(S) > C$, dan kan door codering $H(S/B)$ willekeurig dicht bij $H(S) - C$ gebracht worden.

toelichting bij equivocatie:



Opm: Shannon zegt dus dat er methoden te ontwerpen zijn waarmee $I(SB)$ bij de ontvanger kan worden afgezonderd van $H(B/S)$

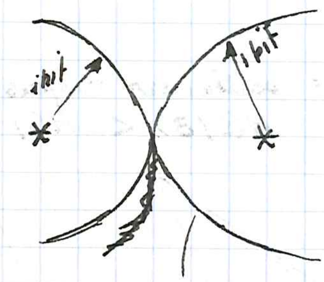
Kanaalcodering

Foutdetecterende code

Bij enkele fouten in het blok kan volstaan worden met 1 pariteitsbit waardoor de Hammingafstand 2 wordt
De Hammingafstand van een kanaalcodewoord is het minimale aantal bits dat in een willekeurige codewoord gewijzigd moet worden om een ander codewoord te krijgen
Zonder pariteitsbit is in het algemeen de H.A. gelijk aan 1

0 P. HA → 1

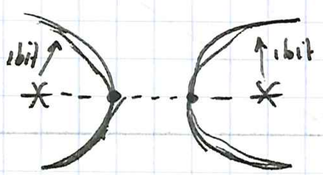
1 P. HA → 2



* toegestane codewoorden

niet-toegestane codewoorden

nu Hammingafstand 3



geeft zondermeer correctie voor enkelvoudige fouten of detectie voor enkel en dubbelvoudige fouten dubbele fout detectie

enkele fout correctie

$HA = 4$

x . . . x

enkelv. fout correctie +
dubbele fout detectie

of

1; 2; 3- voudige foutcorrectie

<u>Foutcorrectie</u> (<u>enkelvoudige</u> fouten in het blok)

<u>Hamming</u> : 3 info- bits $\longrightarrow$ 4 gebeurtenissen
(alles goed + 3 versch. fouten)

$\rightarrow$ 4 codewoorden nodig (syndroom)

$\rightarrow$ 2 pariteitsbits $\longrightarrow$ <u>worden 5 bits</u>

5 bits $\rightarrow$ 6 gebeurtenissen (syndromen) $\rightarrow$ 3 p.bits
dus 1 extra
om 2 p.bits te besch.

6 bits $\rightarrow$ 7 geb $\rightarrow$ 7 syn $\rightarrow$ 3 bits

1 syndroom over dus aantal info-bits uit te breiden naar 4

Eis : bij <u>m</u> pariteitsbits

$$2^m \geq n+1$$ alles goed

waarin $n = k+m$ $\quad k$ = aantal info bits

$\rightarrow$ beschikbare syndromen $\geq$ nodige syndromen

aantal x 0 bits fout - - - - - - - aantal hier n bits fout
in m bits

$$\binom{m}{0} + \binom{m}{1} + \binom{m}{2} - - - \binom{m}{n}$$

Efficient : ~~?~~ gelijktekenen

n	m
3	2
7	3
15	4
31	5

(7,4) - code
(15,11) - code

Ontwerp van (7,4) — code
afspraak: Indicatie in de N.B.C.

PCB3 PCB2 PCB1 (syndroom)			
PCB3	PCB2	PCB1	
0	0	0	alles goed
0	0	1	bit 1 fout
0	1	0	
0	1	1	
1	0	0	
1	0	1	
1	1	0	
1	1	1	bit 7 fout

PCB 1 = $1 \oplus 3 \oplus 5 \oplus 7$ hierbij PB1
PCB 2 = $2 \oplus 3 \oplus 6 \oplus 7$ " PB2
PCB 3 = $4 \oplus 5 \oplus 6 \oplus 7$ " PB3

bits 1 2 en 4 zijn de pariteitsbits
deze beïnvloeden namelijk exclusief hun eigen
mod. 2 - som

VB: info woord 1011 even parity

7	6	5	4	3	2	1
1	0	1	0	1	0	1

kanaal.

7	6	5	4	3	2	1
1	0	0	0	1	0	1

PCB 1 = $1 \oplus 1 \oplus 0 \oplus 1 = 1$

PCB 2 = $0 \oplus 1 \oplus 0 \oplus 1 = 0$

PCB 3 = $0 \oplus 0 \oplus 0 \oplus 1 = 1$

syndroom 101 $\rightarrow$ 5 beschadigd

Opgave ga na dat voor correctie van max T fouten een (n, k)-code nodig is met

$$2^{n-k} \geq \sum_{i=0}^{T} \binom{n}{i}$$

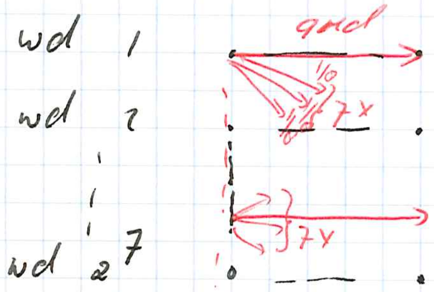
Hammingcodes kunnen eenvoudig uitgebreid worden tot code met H. A. = 4 door toevoegen van 1 bit

We voegen een pariteitsbit toe over het gehele H.C-woord

syndroom	PCB+	
$= 0$	0	geen fout
$= 0$	1	PCB+ is zelf fout
$\neq 0$	0	dubbele fout (detectie)
$\neq 0$	1	enkele fout (correctie)

Het voorbeeld van Shannon

Binair kanaal: in blok van 7 bits precies 1 fout / geen fout. Bezien we nu de 7e uitbreiding



! alle gebeurtenissen zijn even waarschijnlijk
! kanaal is dus uniform

$$C = \max(H(B)) - H(C) \quad /* \text{ uniform kanaal } */$$
$$= \log 2^7 - 8 \cdot \tfrac{1}{8} \log 8$$
$$= 7 - 3 = 4 \text{ bit / blok}$$

Neem een Hammingcode (7, 4), foutloze transmissie op de capaciteit

Verbetering door de toepassing van Hamming-code op B.S.C. met foutkans p

k infobits en m pariteitsbits

1) zonder codering

foutkans : 1 − kans op alles goed

$$= 1 - (1-p)^k$$

$$= 1 - \left\{ \binom{k}{0} p^0 - \binom{k}{1} p^1 \pm \cdots (\pm) \binom{k}{k} p^k \right\}$$

$$\approx 1 - \left(1 - kp + \frac{k(k-1)}{2} \cdot p^2 - \cdots \right)$$

$$\approx kp - \frac{k(k-1)}{2} p^2$$

2) met codering

foutkans : 1 − kans op alles goed − kans op 1 fout

$k+m=n$

$$= 1 - (1-p)^n - \binom{n}{1} p \cdot (1-p)^{n-1}$$

$$= 1 - \left[1 - np + \frac{n(n-1)}{2} p^2 \right] - np \left[\binom{n-1}{0} p^0 + - \binom{n-1}{1} p^1 + \binom{n-1}{2} p^2 - \cdots \right]$$

$$\approx \cancel{np} - \frac{n(n-1)}{2} p^2 - \cancel{np} + np(n-1)p + - np \cdot \frac{(n-1)(n-2)}{2} p^2$$

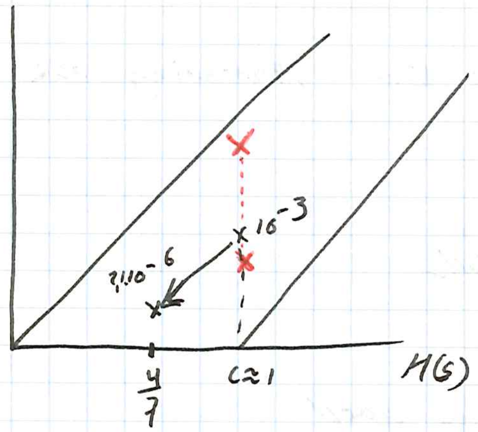
$$\approx \frac{n(n-1)}{2} p^2$$

stel : $p = 10^{-3}$

$k = 4$

$n = 7$

$$\left. \begin{array}{l} kp = 4 \cdot 10^{-3} \\ \frac{n(n-1)}{2} p^2 = 21 \cdot 10^{-6} \end{array} \right\} \text{ merit getal van de code } \frac{4}{21} \cdot 10^3$$



foutkans $: 10^{-3}$ $c \approx 1$

(7, 4)

grotere snelheid t.b.v. handhaven van info-transmissie

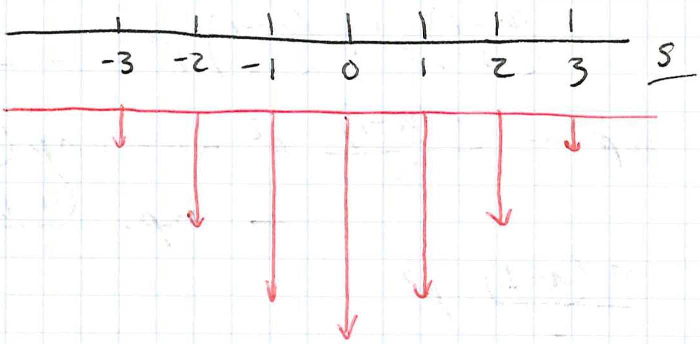
$\longrightarrow$ grotere foutkans

pas als oorspronkelijke $P_{fout} < 10^{-5}$ boeken we reële winst

Continue Bronnen

Hierbij behoort een continue kansverdeling

Discrete verdeling

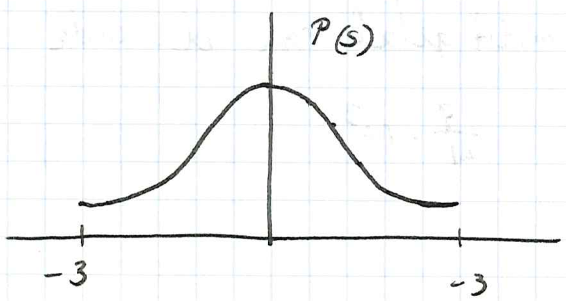


$\Sigma\, p\{s_i\} = 1$

Bij toename van het aantal uitkomsten wordt het aantal pijltjes groter en ze worden korter!

In de limiet (continue) krijgen de pijltjes $\underline{\underline{0}}$!

We moeten dus i.p.v. kansen, kansdichtheden uitzetten

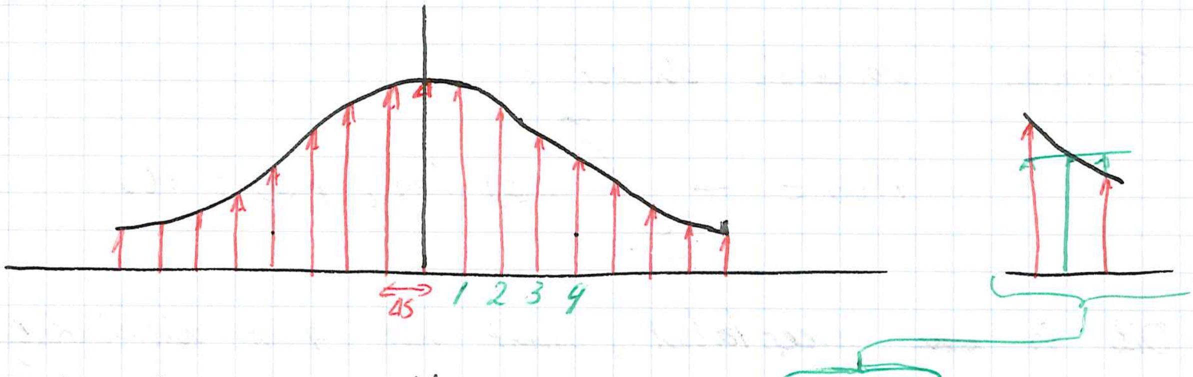


We zetten voor elke s uit de kans dat de uitkomst voor een experiment in een eenheidsinterval rond die s-waarde valt.

Dan: $\displaystyle\int_{-3}^{3} p(s)\,.\,ds = 1$

Nu de entropie bepalen

We verdelen het gebied onder $p(s)$ in een aantal intervallen Δs



We bepalen voor elk interval $p\{s_{midden}\}\,.\,\Delta s$

$$H(s) = -\sum p\{s_{midden}\}\Delta s \,.\, \log\left[p\{s_{midden}\}\,.\,\Delta s\right]$$

$$= -\sum p\{s_{midden}\}\Delta s \,.\, \log\left[p\{s_{midden}\}\right]$$

$$-\sum p\{s_{midden}\}\Delta s\,.\, \log \Delta s$$

Nu Δs naar 0:

$$H(s) = -\int \left(p(s)\ \log\{p(s)\}\right) ds \ +$$

$$-\lim_{\Delta s \to 0} \log \Delta s \,.\, \underbrace{\int p(s)\, d(s)}_{=1}$$

$$H(s) = - \int p\{s\} \log \{p\{s\}\} ds + \infty$$

We introduceren een een andere eenheid voor s i.p.v de willekeurig die gegeven is, nl Δs_{min}, de waarnemingsgrens (drempel. $\underline{\Delta s_{min} = 1}$

Dan wordt 2e term $\underline{\log \Delta s_{min} = \log 1 = 0}$!

Eerste term zou eigenlijk een som moeten blijven met Δs_{min} erin het verschil tussen deze som en de integraal is praktisch verwaarloosbaar

Shannon poneerde direct:

$$H(s) = - \int_{-\infty}^{\infty} p(s) \log \{ p(s) \} ds$$

Dit is ~~een~~ acceptabel, want het gaat uiteindelijk $I(SB)$

$$I(SB) = H(B) - H(B/S)$$

en voor $H(B/S)$ geldt:

$$H(B/S) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p\{B/S\} \log p\{B/S\} \, dB \, ds +$$

$$- \lim_{\Delta B \to 0} \log \Delta B$$

De laatste term komt ook in $H(B)$ voor

Dus correct:

$$I(SB) = -\int_{-\infty}^{\infty} p\{B\} \log p\{B\} dB + \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p\{SB\} \log p\{B/S\} dB ds$$

welke functie $p\{B\}$ maakt $H\{B\}$ maximaal !

na vrij complex rekenwerk volgt :

De normale verdeling (gaussische verdeling)

$$p\{B\} = \frac{1}{\sqrt{2\pi}\,\sigma_B} \cdot e^{-\frac{B^2}{2\sigma_B^2}} \quad -(B-\mu)^2$$

(met verwachting nul !)

→ top v.d. verdeling ligt op nul !
=(géén gelijksp - component)

σ_B is standaardafwijking :

$$\sigma_B = \sqrt{\int_{-\infty}^{\infty} B^2 \, p\{B\} \, dB}$$

Het bereikte maximum is :

$$\log \sqrt{2\pi e \, \sigma_B^2}$$

$$= \log \sigma_B . 2{,}047095585$$

$$= \log \sigma_B . 2{,}04709\ldots$$

Nu $H(B/S)$ veroorzaakt door ruis :

neem aan : ruis is normaal verdeeld met verwachting $\underline{0}$,
ruis is additief

$$H(B/S) = H\left(\overset{\text{ruissignaal}}{S+N}/S\right)$$

$$= H(S/S) + H(N/S)$$

$$H(S/S) \to 0 \qquad H(N/S) = H(N)$$

Dus

$$I(SB) = H(B) - H(N)$$

Dus cap:

$$C = (\log \sigma_B + 2{,}047\ldots) - (\log \sigma_N + 2{,}047\ldots)$$

$$= \log \frac{\sigma_B}{\sigma_N}$$

Uit hansreh volgt dat som of verschil uit twee (normaal) verdeelde signalen is weer een normaal verdeeld signaal

En geldt ~~dat~~ dan:

$$\sigma_B = \sqrt{\sigma_S^2 + \sigma_N^2}$$

$$C = \log \frac{\sqrt{\sigma_S^2 + \sigma_N^2}}{\sigma_N}$$

$$= \log \sqrt{1 + \left(\frac{\sigma_S}{\sigma_N}\right)^2}$$

← S/N verhouding

$$= \log \sqrt{\left(1 + \left(\frac{P_s}{P_n}\right)\right)} \text{ bit/sy}$$

Bandbreedte B van het signaal

2B samples / sec.

$$C = 2B \log \sqrt{\left(1 + \frac{P_S}{P_N}\right)} \doteq B \log \left(1 + \frac{P_S}{P_N}\right) \quad \text{bit/sec.}$$

trade-off tussen bandbreedte en signaal-ruis verh.

Vb: Telefoonkanaal $B = 4$ kHz $S/N = 10$ dB

$$\frac{P_S}{P_N} = 10^{\,^{10}\log 10} = 10$$

$C = 4000 \log 11 = 13\,840$ bit/sec

Een nette bron met 13840 bit/sec moet op het kanaal aangepast worden dwz het kanaal transporteert basisfreq 6920 Hz > B
Hiervoor codering nodig. (Signaal „ruiskarakter" geven)

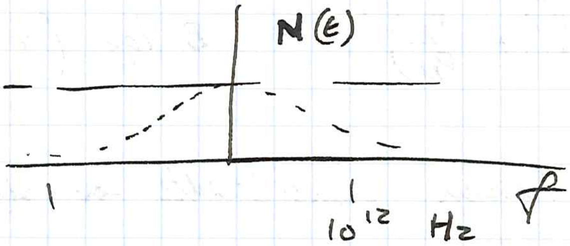
Spraak: 1,5 bit / letter („fonen") klankeenheden

5 lettergrepen van gem 3 letters / sec.

$5 \cdot 3 \cdot 1{,}5 = 22{,}5$ bit / sec.

Op het beschouwde kanaal kunnen dus $\frac{13\,840}{22{,}5} = 615$ gesprekken met in principe willekeurig kleine fouthans

Op kanaal is witte ruis aanwezig dwz met konstante dichtheidspectrum



Bij vergroten van B wordt P_N dus groter
we introduceren ruisvermogen / Hz.

$$\frac{P_N}{B} = P_{N0} \qquad \cancel{B_0}$$

Bandbreedte B_0 waarvoor ruisvermogen gelijk is aan signaal formule $B_0 \cdot P_{N0} = P_S$

$$C = B \log\left(1 + \frac{B_0 \cdot P_{N0}}{B \cdot P_{N0}}\right)$$

$$\frac{C}{B_0} = \frac{B}{B_0} \log\left(1 + \frac{B_0}{B}\right)$$

functie : $y = x \, {}^2\log\left(1 + \frac{1}{x}\right)$

$x = 0 \quad : f(0) = 0$

$x = 1 \quad : f(1) = 1$

afgeleide : na enig rekenwerk volgt

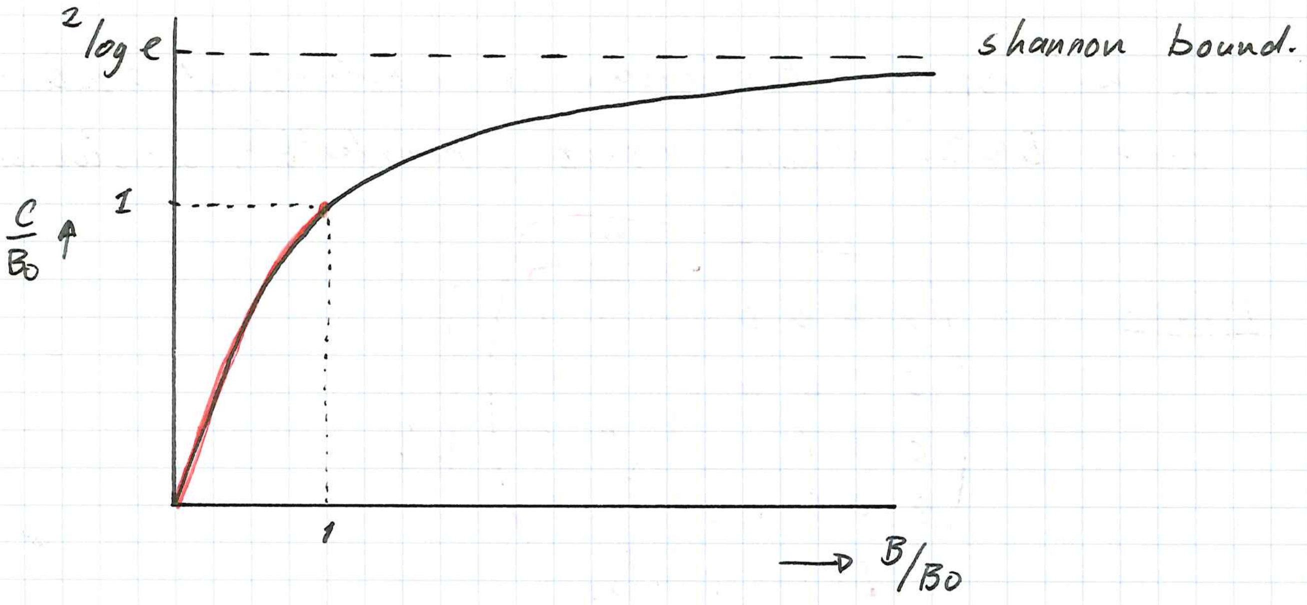
$$y' = {}^2\log\left(1 + \frac{1}{x}\right) + {}^2\log e \, \frac{-1}{x+1}$$

dus

$$\lim_{x\to\infty} \quad \lim_{x\to\infty} \frac{{}^2\log\left(1 + \frac{1}{x}\right)}{\frac{1}{x}} = \lim_{x\to\infty} \frac{{}^2\log e \cdot \frac{1}{1+\frac{1}{x}} \cdot \cancel{\frac{-1}{x^2}}}{\cancel{\frac{-1}{x^2}}}$$

1 0

$$= {}^2\log e \approx 1,442695041$$



Het vergroten van B is alleen zinnig als : $0 \le \frac{B}{B_0} < 1$, daarboven is het verkwisting

<u>Kanaal codering</u> (7, 4) (1024, 890)

Beschrijven van Hamming-coderings en decoderings proces met matrices

(7,4)

7	6	5	4	3	2	1
D_1	D_2	D_3	P_3	D_4	P_2	P_1

$P_1 = 3 \oplus 5 \oplus 7$

$P_2 = 3 \oplus 6 \oplus 7$

$P_3 = 5 \oplus 6 \oplus 7$

coderen

$$(d_1, d_2, d_3, d_4) \cdot \underbrace{\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}}_{\text{code-generator matrix } \underline{G}}$$

optellen = mod 2

In het vervolg beschouwen we uitsluitend systematische code. D.W.Z. databits voorop, pariteitbits achteraan.

Hier:

$$\overbrace{\left(\begin{array}{cccc|ccc} 1&0&0&0&1&1&1\\ 0&1&0&0&1&1&0\\ 0&0&1&0&1&0&1\\ 0&0&0&1&0&1&1 \end{array}\right)}^{n}\Bigg\}\,k$$

$$\underbrace{}_{I_k}\qquad \underbrace{}_{P_{k\times m}}$$

eenheidsmatrix

$$(G) = (I_k,\ P_{k\times m})$$

$$m\left\{\overbrace{\left(\begin{array}{cccc|ccc} 1&1&1&0&1&0&0\\ 1&1&0&1&0&1&0\\ 1&0&1&1&0&0&1 \end{array}\right)}^{n}\right. \cdot \underbrace{\begin{pmatrix} d_1\\ d_2\\ d_3\\ d_4\\ p_3\\ p_2\\ p_1 \end{pmatrix}}_{\bar{c}_{gez.}} = \bar{0}.$$

paritycheck matrix $\Rightarrow H$.

$P^T_{k\times m}$ $\qquad$ I_m.

Dus: $H\cdot\bar{c}_{ontv} = \text{syndroom} = \bar{s}$

$\bar{c}_{ontv} = \bar{c}_{gez} \oplus \bar{e}$ $\qquad$ $\bar{e}$ = errorvector

$\rightarrow$ $H\,\bar{c}_{ontv} = H\{c_{gez} \oplus H.\bar{e} = 0 + H\bar{e} = H\bar{e}$

Cyclische code.

een middel om in de overmaat van mogelijke codes een selectie te maken.

Als: $(c_1, c_2, --, c_{n-1}, c_n)$ een codevector is dan ook

$(c_n, c_1, c_2, ---, c_{n-1})$

***

resumeetje:

G : code generator matrix $\longrightarrow$ $\overline{d} \cdot G = \overline{c}$ zijn alleen „geh0nteld"

H : parity check matrix $\longrightarrow$ $H \cdot \overline{c}^T = \overline{0}$

↳ syndroom = 0

Bij een transmissiefout : $H(\overline{c}^T \oplus \overline{e})$

Vb : $\overline{c} = (1, 0, 1, 1)$

$\overline{c}^T = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$ goed

Vb.

$\overline{c}^T \oplus \overline{e} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \oplus \underbrace{\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}}_{\overline{e}\text{ vector}} = \underbrace{\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}}_{\text{ontvang vector}}$

***

Als $\overline{c}_1 = (c_1, c_2, \ldots, c_n)$ een codewoord is,
dan ook $\overline{c}_2 = (c_2, c_3, \ldots\ldots c_n, c_1)$
G wordt dan :

$$\left(\begin{array}{ccc|ccc} 1 & \cdots & 0 & - & - & - \\ \vdots & \ddots & \vdots & - & - & - \\ & & & - & & - \\ 0 & \cdots & 1 & - & - & \boxed{1} \end{array}\right)$$

hier moet een 1 staan !!

Alle mogelijke k-bits woorden zijn datawoorden
Neem het woord $\overline{d} = (0, 0, \ldots, 0, 1)$, stel dat in aangegeven positie in matrix een 0 voorkomt, dan volgt

$$\overline{c} = (\underbrace{0, 0, 0, \ldots, 0, 1}_{\overline{d}_1} \mid \underbrace{\ldots 0}) $$

dan ook $\overline{c}_2 = (\underbrace{0, 0, \ldots\ldots, 0}_{\overline{d}_2} \mid 1 \ldots)$

$\overline{d}_2$ bevat alleen nullen, dus alle pariteitbits behoren ook nul te zijn $\Longrightarrow$ tegenspraak

In de laatste rij van G behoren minstens twee eenen voor te komen.

We introduceren een polynoom beschrijving van vectoren:

$\overline{c} = (c_1, c_2, ----, c_n)$ wordt nu.

$c(x) = c_1 x^{n-1} + c_2 x^{n-2} + --- + c_{n-1} x + c_n$

waarin x een <u>verschuivingsoperator</u> is. Machten van x zijn dus plaatsbepalens voor de binary digits.
Modulo-2 optelling blijft gehandhaafd bij optelling van polynomen

vb: $\overline{c} = (0111) \oplus \overline{e} = (0010)$

$$c(x) \oplus e(x) = (x^2 + x + 1) \oplus x$$
$$= x^2 + (x \oplus x) + 1$$
$$= x^2 + 1$$

Algemeen: $\boxed{x^i \oplus x^i = 0}$

Bezien we nu: $c(x) . x = c_1 x^n + c_2 x^{n-1} + -- + c_{n-1} x^2 + c_n x$

$$x^4 = 1 = x^4 \mod (x^4 + 1)$$
$$= x^4 \oplus (x^4 + 1) = x^4 \oplus x^4 + 1 = \underline{1}$$

Andere notatie: $x^{(n-1)+a} = \dfrac{x^{(n-1)+a}}{x^n + 1}$

Illustratie

$n = 4 \rightarrow \overline{c_1} = (1101)$ $c_1(x) = x^3 + x^2 + 1$

$\overline{c_2}(x) = \overline{c_1}(x) \cdot x = x^4 + x^3 + x$

$$\begin{array}{l} x^4+1 \ / \ x^4 + x^3 + x \ \backslash \ 1 \\ \qquad\quad \underline{x^4 \qquad\qquad\quad +1} \ \oplus \\ \qquad\quad 0 + x^3 + x + 1 \end{array}$$

$\longrightarrow$ $\overline{c_2} = (1011)$

$c_2(x) = x^3 + x + 1$

$$c_3(x) = x^2 c_1(x)$$
$$= x^5 + x^4 + x^2$$

$$
\begin{array}{l}
x^4+1 \; / \; x^5 + x^4 + x^2 \quad \backslash \; x+1 \\
\quad\;\; x^5 \qquad\qquad\;\; + x \quad \oplus \\
\hline
\qquad\quad x^4 + x^2 + x \\
\qquad\quad x^4 \qquad\quad +1 \quad \oplus \\
\hline
\qquad\qquad x^2 + x + 1 \quad \longrightarrow \bar{c}_3 = (0\,1\,1\,1)
\end{array}
$$

We kunnen nu ook G schrijven als machten van x:

Bv: Hamming (7,4)-code

$$(d_1, d_2, d_3, d_4)\begin{pmatrix} 1\,0\,0\,0 & 1\,1\,1 \\ 0\,1\,0\,0 & 1\,1\,0 \\ 0\,0\,1\,0 & 1\,0\,1 \\ 0\,0\,0\,1 & 0\,1\,1 \end{pmatrix}$$

We schrijven nu:

$$(d_1, d_2, d_3, d_4)\left(\begin{array}{cccc|ccc} x^6 & - & - & - & x^2 & x & 1 \\ - & x^5 & - & - & x^2 & x & - \\ - & - & x^4 & - & x^2 & - & 1 \\ - & - & - & x^3 & - & x & 1 \end{array}\right)$$

Vervangen we de matrix door polynoomvectoren

$$(d_1, d_2, d_3, d_4)\begin{pmatrix} x^6 + x^2 + x + 1 \\ x^5 + x^2 + x \\ x^4 + x^2 + 1 \\ x^3 + x + 1 \end{pmatrix}$$

$$= d_1(x^6 + x^2 + x + 1) \oplus d_2(x^5 + x^2 + x) \oplus d_3(x^4 + x^2 + 1) \oplus d_4(x^3 + x + 1)$$
$$= d_1 \cdot x^6 + d_2 \cdot x^5 + d_3 \cdot x^4 + d_4 \cdot x^4 + x^2(d_1 \oplus d_2 \oplus d_3) +$$
$$+ x(d_1 \oplus d_2 \oplus d_4) +$$
$$+ (d_1 \oplus d_3 \oplus d_4)$$

Polynoom in de laatste rij is het generator polynoom,

hier in vb dus: $g(x) = x^3 + x + 1$

Bezien we de cyclische codes (merk op: $\bar{d}$ is altijd cyclisch) neem :

$$d_1 = (0,0,0,1) \begin{pmatrix} \equiv \\ g(x) \end{pmatrix} = g(x)$$

$$d_2 = (0,0,1,0) \begin{pmatrix} \equiv \\ g_1(x) \\ g(x) \end{pmatrix} = g_1(x) \qquad \text{neem aan : } g_1(x) = x\, g(x)$$

$$d_3 = g_2(x) = x^2 \cdot g(x)$$

Algemeen :

$$(d_1 \text{ - - - - - } d_k) \begin{pmatrix} x^{k-1} \cdot g(x) \\ \vdots \\ x \cdot g(x) \\ g(x) \end{pmatrix} = c(x)$$

ofwel :

$$g(x) \cdot \{ d_1 x^{k-1} + \text{---} + d_{k-1} x + d_k \} = c(x)$$

$$g(x) \cdot d(x) = c(x)$$

De zo verkregen code is <u>niet</u> systematisch

bv: $g(x) = x^3 + x + 1$ (7,4)-code $\bar{d} = (1010)$

$$c(x) = (x^3 + x)(x^3 + x + 1)$$

$$= x^6 + \cancel{x^4} + x^3 + \cancel{x^4} + x^2 + x$$

$$= x^6 + x^3 + x^2 + x$$

$$\bar{c} = (1001110)$$

Opm : ook $g(x) = x^3 + x^2 + 1$ geeft een (7,4)-cyclische code

Voor het gegeven voorbeeld dus

$$G = \left(\begin{array}{cccc|ccc} x^6 & - & x^4 & x^3 & - & - & - \\ - & x^5 & - & x^3 & x^2 & - & - \\ - & - & x^4 & - & x^2 & x & - \\ - & - & - & x^3 & - & x & 1 \end{array}\right)$$

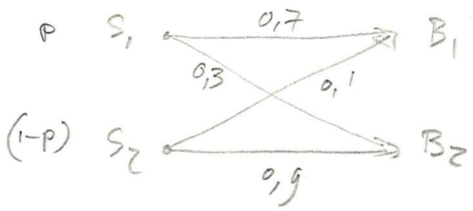
hier <u>geen</u> I-matrix dus code <u>niet</u> systematisch

INT opgaven

feb 07/2

Binair kanaal $\begin{bmatrix} 0,7 & 0,3 \\ 0,1 & 0,9 \end{bmatrix} = T$

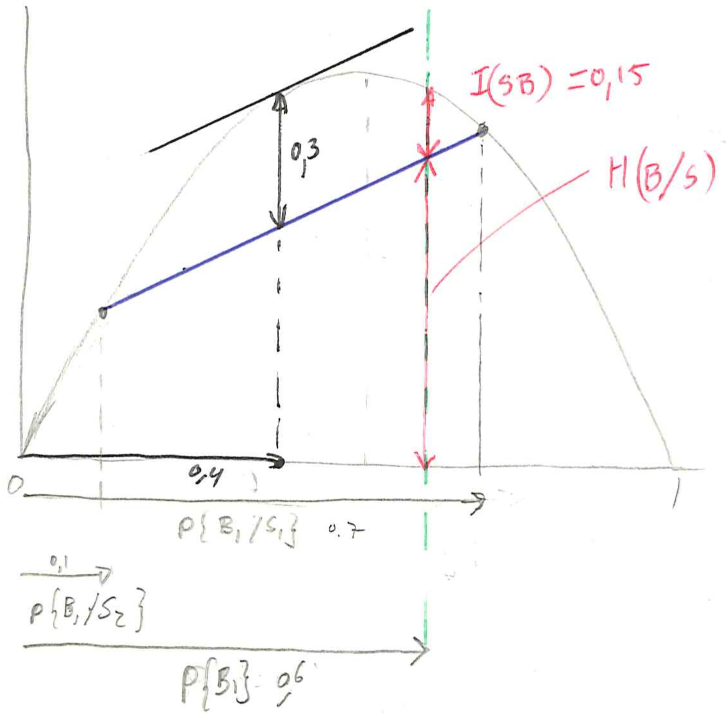
Bronsymbolen S_1, S_2



$p\{B_2\} = p \cdot 0,3 + (1-p)\, 0,9 = 0,4.$

$-0,6p + 0,9 = 0,4$

$0,6p = \frac{1}{2} \Rightarrow p = 5/6$

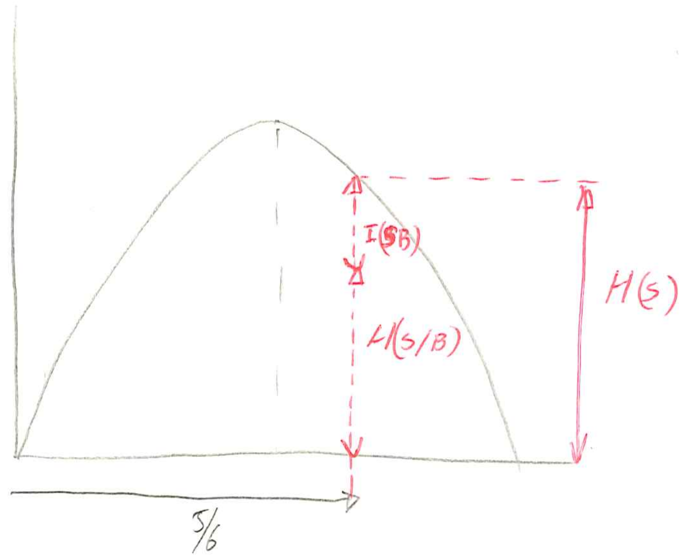


$p\{B_1\} = 0,4$

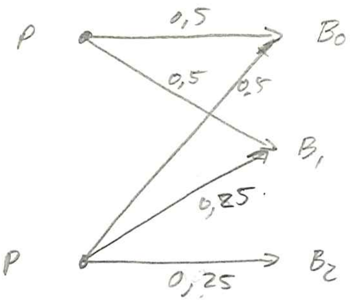
dus: $p \cdot 0,7 + (1-p)\, 0,1 = 0,4$

↓

Bronkans.



88/2



$p\{B_0\} = 0{,}5\,p + 0{,}5(1-p) = 0{,}5$

$p\{B_1\} = 0{,}5\,p + 0{,}25(1-p) = 0{,}25 + 0{,}25\,p$

$p\{B_2\} = 0{,}25\,(1-p)$

gegeven

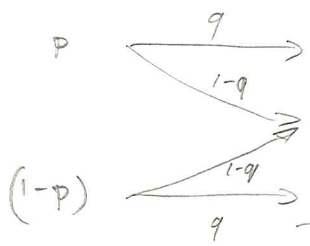
$p = \frac{1}{2}$: $\quad H(B) = \frac{1}{2}\log 2 + \frac{3}{8}\log \frac{8}{3} + \frac{1}{8}\log 8$

$\sum P\{B_i\} \log 1/P\{B_i\}$

$$I(SB) = \underbrace{\left[\frac{1}{2}\log 2 - \frac{1}{4}(1+p)\log\frac{1+p}{4} - \frac{1}{4}(1-p)\log\left(\frac{1-p}{4}\right)\right]}_{H(B)}$$

$$- \underbrace{\left[p\cdot\frac{1}{2}\log 2 + p\cdot\frac{1}{2}\log 2 + (1-p)\cdot\frac{1}{2}\log 2 + (1-p)\frac{1}{4}\log 4 + (1-p)\frac{1}{4}\log 4\right]}_{H(B/S)}$$

diff $\to 0 \Rightarrow p = \frac{3}{5}$



$I(SB) = H(S)\cdot q$

$\to C = Q$

Shannon

blok 7 symbolen 1 of geen fout

8 geb

Alles goed.
Bit 1 fout
⋮
Bit 7 fout

} even waarschijnlijk

$C = [\max H(B)] - H(C)$

$= \log 2^7 - 8 \cdot 1/8 \log 8$

$= 7 - 3 = 4$

4 bit / sym van de 7e uitbreiding

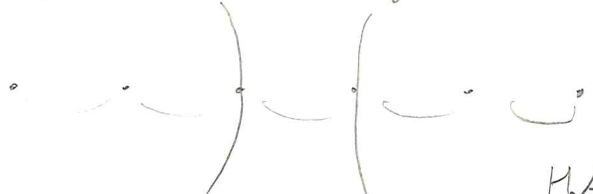
(7,4) Hamming → Tr. snelheid 4 bit/sym $= \underline{\underline{C}}$

feb 87 (10,4)

$2^6 \geq 1 + 10 + \binom{10}{2}$ $\quad \left\{ \sum_{0}^{T} \binom{n}{i} \right\}$ T fouten $\quad \binom{10}{2}$

$64 \geq 1 + 10 + 45$ klopt

dubbele fouten kunnen gekorrigeerd worden

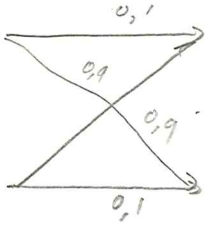


H.A. = 5

3c

o o
* o
o x } transmissie gelukt
x x → fout

↳ foutkans $= (0{,}1)^2 = 0{,}01$



foutkans = 0,1

2 x zenden

foutkans $\rightarrow (0,1)^2 + \frac{1}{2}[0,1 \cdot 0,9 + 0,9 \cdot 0,1]$

$= 0,01 + 0,09 = 0,1$

000 $\longrightarrow$

000	0	$\rightarrow$ alles
001	0	
010	0	
011	1	
100	0	
101	1	
110	1	
101	1	
111	0	$\rightarrow$ alles

foutkans : $3 \cdot 0,9 \cdot (0,1)^3 + (0,1)^3$

0,028