Coderingstheorie

Een toepassing van lineaire algebra

F.Beukers

Het probleem

0 0 1 1 0 1 1 1 0 0 1 0 1 1 1 0 1

Het probleem

0 0 1 1 0 1 1 1 0 0 1 0 1 1 1 0 1

0 0 1 1 0 1 1 0 0 0 1 0 1 1 0 0 1

Het probleem

0 0 1 1 0 1 1 1 0 0 1 0 1 1 1 0 1

0 0 1 1 0 1 1 0 0 0 1 0 1 1 0 0 1

0 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1

Het probleem

0 0 1 1 0 1 1 1 0 0 1 0 1 1 1 0 1

0 0 1 1 0 1 1 0 0 0 1 0 1 1 0 0 1

0 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1

Vermoedelijk juiste bericht:

0 0 1 1 0 1 1 1 0 0 1 0 1 1 0 0 1

Informatieverhouding in dit voorbeeld:

$$\frac{\text{Lengte van informatie}}{\text{Lengte verstuurde boodschap}} = \frac{1}{3}$$

U KUNT DIF BERIQT LGZEN OMDAW ER OVERTOLMIGE INFOSMATIE ACNWEZIG IS

U KUNT DIF BERIQT LGZEN OMDAW ER OVERTOLMIGE INFOSMATIE ACNWEZIG IS

Aantal mogelijke woorden van vijf letters:

$$26 \times 26 \times 26 \times 26 \times 26 = 11881376$$

U KUNT DIF BERIQT LGZEN OMDAW ER
OVERTOLMIGE INFOSMATIE ACNWEZIG IS

Aantal mogelijke woorden van vijf letters:

$$26 \times 26 \times 26 \times 26 \times 26 = 11881376$$

In digitale techniek bestaan woorden uit het alfabet $0, 1$,
de binaire woorden

IDEE:

Maak zelf een woordenboek bestaande uit binaire woorden.
Noem dit de code woorden.
Verstuur de informatie met behulp van deze codewoorden.

Check sums

In computergeheugens:

0	0	1	0	1	0	1	1	0
1	0	0	0	1	0	0	1	1

Laatste cijfer van ISBN-nummers. Voorbeeld, ISBN 0-8436-1072-7

$$
\begin{array}{rcl}
10 \times 0 & = & 0 \\
9 \times 8 & = & 72 \\
8 \times 4 & = & 32 \\
7 \times 3 & = & 21 \\
6 \times 6 & = & 36 \\
5 \times 1 & = & 5 \\
4 \times 0 & = & 0 \\
3 \times 7 & = & 21 \\
2 \times 2 & = & 4 \\
1 \times 7 & = & 7 \\
\hline
\text{Totaal:} & & 198 = 11 \times 18
\end{array}
$$

Voorbeeld: [7,4] binaire Hamming code

0	0	0	0	$\rightarrow$	0	0	0	0	0	0	0
1	0	0	0	$\rightarrow$	1	0	0	0	0	1	1
0	1	0	0	$\rightarrow$	0	1	0	0	1	0	1
0	0	1	0	$\rightarrow$	0	0	1	0	1	1	0
0	0	0	1	$\rightarrow$	0	0	0	1	1	1	1
1	1	0	0	$\rightarrow$	1	1	0	0	1	1	0
1	0	1	0	$\rightarrow$	1	0	1	0	1	0	1
1	0	0	1	$\rightarrow$	1	0	0	1	1	0	0
0	1	1	0	$\rightarrow$	0	1	1	0	0	1	1
0	1	0	1	$\rightarrow$	0	1	0	1	0	1	0
0	0	1	1	$\rightarrow$	0	0	1	1	0	0	1
1	1	1	0	$\rightarrow$	1	1	1	0	0	0	0
1	1	0	1	$\rightarrow$	1	1	0	1	0	0	1
1	0	1	1	$\rightarrow$	1	0	1	1	0	1	0
0	1	1	1	$\rightarrow$	0	1	1	1	1	0	0
1	1	1	1	$\rightarrow$	1	1	1	1	1	1	1

Elk tweetal code-woorden heeft onderlinge afstand ≥ 3.

Informatieverhouding is $\frac{4}{7}$

Stel binnengekomen:

$0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0$

Woord uit onze code corresponderend met $0\ 1\ 0\ 1$

Informatieverhouding is $\frac{4}{7}$

Stel binnengekomen:

0 1 0 1 0 1 0

Woord uit onze code corresponderend met 0 1 0 1

Stel binnengekomen:

1 1 1 1 0 0 0

Geen woord uit onze code, wel afstand 1 tot:

1 1 1 0 0 0 0

corresponderend met 1 1 1 0

Foutendetecterende matrix

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

Voorbeeld van foutendetectie:

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

STELLING VAN SHANNON (1948)

Stel we hebben een communicatiekanaal met kans p of verkeerde doorgave. Kies een vast getal $R < 1$ en een zeer kleine tolerantie t. Dan is er een foutencorrigerende binaire code met informatieverhouding minstens R waarvan de kans op fouten, na foutencorrectie, kleiner dan t is.

Dit kan gerealiseerd worden door de lengte van de codewoorden voldoende groot te maken. Helaas geeft de stelling geen daadwerkelijke constructie van zulke codes.

(Eigenlijk moet gelden:
$R < 1 + p \log p + (1-p) \log(1-p)$.)