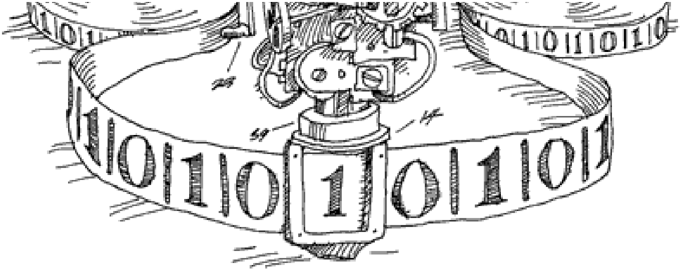
Theoretische Grundlagen der Informatik

Tutorium 13

Institut für Kryptographie und Sicherheit



Kanalkapazität

Die Kanalkapazität bezeichnet maximale Bitrate eines Kanals, bei der eine fehlerfreie Übertragung möglich ist.
Mit einer geeigneten Kodierung kann diese Bitrate näherungsweise erreicht werden.

Definition

Die Kapazität C eines Kanals mit Sender X und Empfänger Y ist

$$C = \max_X I(X;Y) \tag{1}$$

Die Kapazität eines Kanals ist also unabhängig von einem konkreten Sender zu bestimmen. Die Kapazität ist so zu sagen die Transinformation $I(X;Y)$ der (für diesen Kanal) besten Quelle X.

Aufgabe B13 A1

Gegeben sei ein binärer Kanal mit Sender X und Empfänger Y, genannt Z-Kanal, durch die folgende Matrix:

$$Q = \begin{pmatrix} P(Y=0|X=0) & P(Y=0|X=1) \\ P(Y=1|X=0) & P(Y=1|X=1) \end{pmatrix} = \begin{pmatrix} 1 & 0.5 \\ 0 & 0.5 \end{pmatrix}$$

Bestimmen Sie die Kanalkapazität!

Hinweis: Sie können dabei folgendes verwenden:

$$\frac{\log_b x}{dx} = \frac{1}{x \cdot \ln b}$$

Systematische Codes

Damit überprüft werden kann, ob ein Wort richtig übertragen wurde, müssen zusätzlich Daten übermittelt werden.
Eine Möglichkeit der Fehlerprüfung ist die Verwendung von Generatormatrizen.
Dabei werden Wörter der festen Länge k mit Wörter der Länge k+r kodiert. Dazu wird eine Generatormatrix der Form

$$G = \left(\frac{I_k}{A} \right)$$

verwendet, wobei I_k die $k \times k$-Einheitsmatrix ist und A eine $r \times k$-Matrix.
Das kodierte Wort ω_{codiert} erhält man aus dem dazugehörigen Wort ω mittels der Formel $G\omega = \omega_{\text{codiert}}$.

Systematische Codes

Zu der Generatormatrix gehört eine Prüfmatrix

$$H = (A|I_r)$$

mit deren Hilfe sich das Syndrom $s = H\omega_{\text{codiert}}$ ausrechnen lässt.
Ist $s = 0$, wurde die Information im Rahmen der Fehlerkorrektur richtig übertragen. Ist $s \neq 0$ vergleicht man s mit den Spalten von H.
Sei H_k die k-te Spalte von H.

- Gilt $H_k = s$ für exakt ein k, dann ist das k-te Bit im gesendeten Wort falsch.
- Gilt $H_k = s$ für mehrere k, dann ist eine ungerade Anzahl der dazugehörigen Bits falsch.
- Gilt $H_k \neq s$ für alle k, dann sind definitiv mehrere Bits falsch übertragen worden.

Aufgabe B13 A2

Sei $\mathcal{C}$ ein binärer Code, der durch die folgende Generatormatrix gegeben ist:

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

Dekodieren Sie die folgenden empfangenen Wörter!

1. $w_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$
2. $w_2 = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$
3. $w_3 = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$

Hamming-Code

- Eine Codierung zur Erkennung von bis zu 2-bit-Fehlern und Korrektur von 1-bit-Fehlern
- n Paritätsbits sichern 2^n bits - 1 (Code für Fehlerfrei) - n

Hamming-Code

- Eine Codierung zur Erkennung von bis zu 2-bit-Fehlern und Korrektur von 1-bit-Fehlern
- n Paritätsbits sichern 2^n bits - 1 (Code für Fehlerfrei) - n

Bildlich:

$p_1\ p_2\ d_3$

$p_1\ p_2\ d_3$

$p_1\ p_2\ d_3$

Hamming-Code

- Eine Codierung zur Erkennung von bis zu 2-bit-Fehlern und Korrektur von 1-bit-Fehlern
- n Paritätsbits sichern 2^n bits - 1 (Code für Fehlerfrei) - n

Bildlich:

$p_1\ p_2\ d_3\ p_4\ d_5\ d_6\ d_7$

$\color{red}{p_1}\ p_2\ \color{red}{d_3}\ p_4\ \color{red}{d_5}\ d_6\ \color{red}{d_7}$

$p_1\ \color{red}{p_2}\ \color{red}{d_3}\ p_4\ d_5\ \color{red}{d_6}\ \color{red}{d_7}$

$p_1\ p_2\ d_3\ \color{red}{p_4}\ \color{red}{d_5}\ \color{red}{d_6}\ \color{red}{d_7}$

Hamming-Code

- Eine Codierung zur Erkennung von bis zu 2-bit-Fehlern und Korrektur von 1-bit-Fehlern
- n Paritätsbits sichern 2^n bits - 1 (Code für Fehlerfrei) - n

Bildlich:

$$p_1\ p_2\ d_3\ p_4\ d_5\ d_6\ d_7\ p_8\ d_9\ d_{10}\ d_{11}\ d_{12}\ d_{13}\ d_{14}\ d_{15}$$

$$\color{red}{p_1}\ p_2\ \color{red}{d_3}\ p_4\ \color{red}{d_5}\ d_6\ \color{red}{d_7}\ p_8\ \color{red}{d_9}\ d_{10}\ \color{red}{d_{11}}\ d_{12}\ \color{red}{d_{13}}\ d_{14}\ \color{red}{d_{15}}$$

$$p_1\ \color{red}{p_2}\ \color{red}{d_3}\ p_4\ d_5\ \color{red}{d_6}\ \color{red}{d_7}\ p_8\ d_9\ \color{red}{d_{10}}\ \color{red}{d_{11}}\ d_{12}\ d_{13}\ \color{red}{d_{14}}\ \color{red}{d_{15}}$$

$$p_1\ p_2\ d_3\ \color{red}{p_4}\ \color{red}{d_5}\ \color{red}{d_6}\ \color{red}{d_7}\ p_8\ d_9\ d_{10}\ d_{11}\ \color{red}{d_{12}}\ \color{red}{d_{13}}\ \color{red}{d_{14}}\ \color{red}{d_{15}}$$

$$p_1\ p_2\ d_3\ p_4\ d_5\ d_6\ d_7\ \color{red}{p_8}\ \color{red}{d_9}\ \color{red}{d_{10}}\ \color{red}{d_{11}}\ \color{red}{d_{12}}\ \color{red}{d_{13}}\ \color{red}{d_{14}}\ \color{red}{d_{15}}$$

Beispiel

1100110 S

Beispiel

1100110	S
1100110	0

Beispiel

1100110	S
1100110	0
1100110	0

Beispiel

1100110	S
1100110	0
1100110	0
1100110	0

Beispiel

1100110	S
1100110	0
1100110	0
1100110	0

$\Rightarrow$ Keine Fehler! Datenwort = 0110

Beispiel

Karlsruher Institut für Technologie

1100110	S
1100110	0
1100110	0
1100110	0

$\Rightarrow$ Keine Fehler! Datenwort = 0110

1100010	S

Beispiel

1100110 S
1100110 0
1100110 0
1100110 0
⇒ Keine Fehler! Datenwort = 0110

1100010 S
1100010 1

Beispiel

1100110	S
1100110	0
1100110	0
1100110	0

$\Rightarrow$ Keine Fehler! Datenwort = 0110

1100010	S
1100010	1
1100010	0

Beispiel

1100110	S
1100110	0
1100110	0
1100110	0

$\Rightarrow$ Keine Fehler! Datenwort = 0110

1100010	S
1100010	1
1100010	0
1100010	1

Beispiel

1100110	S
1100110	0
1100110	0
1100110	0

$\Rightarrow$ Keine Fehler! Datenwort = 0110

1100010	S
1100010	1
1100010	0
1100010	1

$\Rightarrow$ Fehler an der Stelle $2^1 + 2^2 = 5$

Korrektur: 1100110

$\Rightarrow$ repariertes Datenwort: 0110

Aufgabe B13 A3

Karlsruher Institut für Technologie

Gegeben sei der $[7,4]$-Hamming-Code $\mathcal{C}_H$ mit der Erzeugermatrix

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

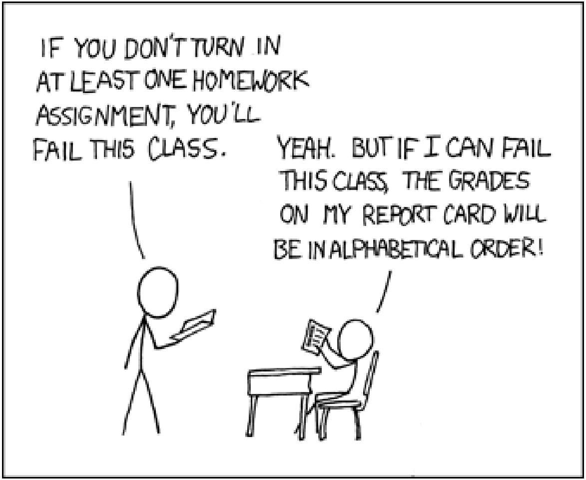
und der Prüfmatrix

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

Dekodieren Sie die folgenden empfangenen Wörter!

1. $w_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$
2. $w_2 = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$
3. $w_3 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$
4. $w_4 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$

Bis zum nächsten Mal!



Lizenzen