Informations– und Kodierungstheorie

1 Entropie als Informationsmaß

Information ist beseitigte Unbestimmtheit.

Die **Entropie** H_i eines Ereignisses x_i mit der Auftrittswahrscheinlichkeit $p(x_i) =: p_i$ ist ein Maß für die Unbestimmtheit von x_i (vor dessen Auftreten) und gleichzeitig seines Informationsgehaltes (nach dessen Auftreten).

$$H_i := \operatorname{ld} \frac{1}{p_i} = -\operatorname{ld} p_i$$

Die Maßeinheit der Entropie ist $\frac{\text{bit}}{\text{Zeichen}}$, $\frac{\text{bit}}{\text{Meßwert}}$ o. ä., manchmal auch nur bit.

2 Diskrete Quellen

2.1 Diskrete Quellen mit unabhängigen Ereignissen

Eine Quelle mit dem Alphabet $X = \{x_1, x_2, \ldots, x_N\}$ mit $\sum_{i=1}^{N} p_i = 1$ wird als **diskrete Quelle X** mit **unabhängigen** Ereignissen bezeichnet.

Die Quellenentropie (mittlerer Entscheidungsgehalt) ist der durch die Auftrittswahrscheinlichkeiten gewichtete Mittelwert aller Entropien H_i:

$$H_m = \sum_{i=1}^{N} p_i H_i = -\sum_{i=1}^{N} p_i \operatorname{ld} p_i$$

Die Entropie wird maximal, wenn alle Ereignisse gleichwahrscheinlich sind. Dies ist der **Entscheidungsgehalt** $H_0 = \operatorname{ld} N$ der Quelle X.

2.2 Diskrete Quellen mit abhängigen Ereignissen (Markow–Quellen)

Bei diesem Modell ist die Auftrittswahrscheinlichkeit eines Ereignisses nicht konstant, sondern von den vorangegangenen m Ereignissen abhängig. → Markow–Quelle m–ter Ordnung. Hier: Beschränkung auf 1. Ordnung.

Die **Übergangswahrscheinlichkeit** $p(x_j|x_i) =: p_{ij}$ gibt die Wahrscheinlichkeit an, mit der das Ereignis x_j nach dem Ereignis x_i auftritt. Diese müssen (im Gegensatz zu den Zustandswahrscheinlichkeiten) zeitlich konstant sein.

Ergodische Markow–Quellen gehen mit fortschreitender Zeit in einen **stationären Zustand** über, d. h. die Zustandswahrscheinlichkeiten sind dann konstant ($\rightarrow p_i^{(t\to\infty)} =: \overline{p_i}$).

Zustandswahrscheinlichkeit zum Zeitpunkt t: $p_j^{(t)} = \sum_{i=1}^{N} p_i^{(t-1)} p_{ij}$

Entropie: $H_m^{(t)} = -\sum_{i=1}^{N} \left(p_i^{(t)} \sum_{j=1}^{N} p_{ij} \operatorname{ld} p_{ij} \right)$ Markow–Entropie: $H_M = -\sum_{i=1}^{N} \left(\overline{p_i} \sum_{j=1}^{N} p_{ij} \operatorname{ld} p_{ij} \right)$

2.3 Verbundquellen

Betrachtung zweier diskreter, unabhängiger Quellen X und Y. Ein Ereignis x_i der Quelle X löst unmittelbar ein Ereignis y_j in der Quelle Y mit der Wahrscheinlichkeit $p(y_j|x_i)$ (**Verbundwahrscheinlichkeit**) aus. Dies wird als **Verbundereignis** (x_i, y_j) der **Verbundquelle** (X, Y) bezeichnet.

$$p(x_i, y_j) = p(x_i) \cdot p(y_j|x_i)$$

Einzelwahrscheinlichkeiten: $p(x_i) = \sum_{j=1}^{M} p(x_i, y_j) \qquad p(y_j) = \sum_{i=1}^{N} p(x_i, y_j)$

Entropie: $H(X,Y) = -\sum_{i=1}^{N}\sum_{j=1}^{M} p(x_i, y_j) \operatorname{ld} p(x_i, y_j)$.

Bedingte Entropie: $H(Y|X) = -\sum_{i=1}^{N}\sum_{j=1}^{M} p(x_i) \cdot p(y_j|x_i) \operatorname{ld} p(y_j|x_i)$.

$\Rightarrow H(X,Y) = H(X) + H(Y|X)$

3 Kodierung diskreter Quellen

3.1 Dekodierbarkeit

Ein Kode ist dekodierbar gdw. er **präfixfrei** ist, d. h. kein Wort ist Anfang eines anderen Wortes. Eine notwendige Bedingung ist die KRAFTsche Ungleichung:

$$\sum_i 2^{-l_i} \leq 1 \quad (l_i\text{: Länge des i-ten Wortes})$$

3.2 Koderedundanz

$$R_K = l_m H_k - H_m$$

l_m: mittlere Kodewortlänge, H_k: Entropie eines Kodezeichens (bei Binärkodierung ist $H_k = 1\,\text{bit}$), H_m: Quellenentropie.

3.3 Quellenkodierung nach Shannon–Fano

- Ordnen der Auftrittswahrscheinlichkeiten der zu kodierenden Quellenzeichen nach fallenden Werten.
- Teilen des geordneten Feldes in zwei Gruppen, so dass die Teilsummen der Wahrscheinlichkeiten in jeder Gruppe möglichst gleich groß sind.
- Kodierung: erste Gruppe: Zeichen 0, zweite Gruppe: Zeichen 1.
- Wiederholung 2. und 3., bis jede Teilgruppe nur noch ein Element enthält.

3.4 Quellenkodierung nach Huffman

- Ordnen des Wahrscheinlichkeitsfeldes nach fallenden Werten.
- Zusammenfassen der letzten zwei Wahrscheinlichkeiten zu einem neuen Wert, korrektes Einordnen entsprechend Schritt 1.
- Wiederholung 2., bis nur noch zwei Elemente vorhanden sind.
- Aufstellen eines Kodebaumes entsprechend dem Reduktionsschema und Zuordnung der Kodesymbole 0 und 1.

4 Kanäle

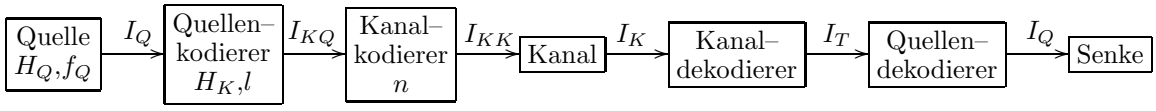
4.1 Bergersches Entropiemodell

Das Modell "Quelle X–gestörter Kanal–Senke Y" kann als Verbundquelle (X, Y) aufgefaßt werden.

$H(X)$	Entropie am Kanaleingang
$H(Y)$	Entropie am Kanalausgang
H_T	Transinformation (Informationsmenge, die im Mittel durch ein Kanalzeichen übertragen wird)
$H(X\|Y)$	Äquivokation (Rückschlußentropie; Anteil der Quelleninformation, die durch Störungen verloren geht; verbleibende Unbestimmtheit über gesendete Information bei Kenntnis der empfangenen Information)
$H(Y\|X)$	Irrelevanz (Entropie, die durch Störungen zusätzlich zur Transinformation empfangen wird)

$$H_T = H(X) - H(X|Y) = H(Y) - H(Y|X)$$

4.2 Diskrete Kanäle



H_Q		$^{bit}/_{QZ}$	Quellenentropie, N Quellzeichen
f_Q		$^{QZ}/_{s}$	Quellensymbolfrequenz
I_Q	$= f_Q H_Q$	$^{bit}/_{s}$	Quelleninformationsfluß
H_K	$=$ ld N	$^{bit}/_{KZ}$	Entropie der Kanalzeichen
l	$= \lceil \frac{H_Q}{H_K} \rceil$	$^{KZ}/_{QZ}$	Anzahl der Kanalzeichen pro Quellzeichen
I_{KQ}	$= f_Q l H_K$	$^{bit}/_{s}$	Quellenkodeinformationsfluß
n	$= l + \Delta l$	$^{KZ}/_{QZ}$	Anzahl der Kanalzeichen pro Quellzeichen (nach Hinzufügen von Redundanz zur Störsicherheit)
I_{KK}	$= f_Q n H_K$	$^{bit}/_{s}$	Kanalkodeinformationsfluß
I_K	$= I_{KQ}$ bzw. I_{KK}	$^{bit}/_{s}$	Kanalinformationsfluß; entspricht I_{KQ} bei ungesicherter, I_{KK} bei gesicherter Übertragung
$v_{\ddot{U}}$	$= I_K = v_s H_K$	$^{bit}/_{s}$	Übertragungsgeschwindigkeit (Informationsfluß)
v_s		$^{KZ}/_{s}$	Schrittgeschwindigkeit, Kanalsymbolfrequenz (übertragungstechnische Größe; kein Informationsfluß!); Einheit auch in Baud
H_T		$^{bit}/_{KZ}$	Transinformation
I_T	$= v_s H_T$	$^{bit}/_{s}$	Transinformationsfluß

4.2.1 Ungesicherte Übertragung

Kein Kanalkodierer $\Rightarrow I_K = I_{KQ}$, $v_s = \frac{I_{KQ}}{H_K}$, $I_T \leq I_{KQ}$

4.2.2 Gesicherte Übertragung

Kanalkodierung zur Beseitung des Informationsverlustes auf gestörtem Kanal $\Rightarrow I_T = I_{KQ}$.

$$v_s = \frac{I_T}{H_T} = \frac{I_{KQ}}{H_T} = f_Q \cdot l \cdot \frac{H_K}{H_T} \quad \Rightarrow \quad I_K = v_s H_K = f_Q \cdot l \cdot \frac{{H_K}^2}{H_T} \qquad \Delta l = \frac{H_K}{H_T} - 1$$

4.2.3 Kanalkapazität

Die Kanalkapazität C ist der Maximalwert des Transinformationsflusses: $C = \max I_T = \max v_s H_T$.
Da $v_{s,max}$ durch die Bandbreite B des Kanals bestimmt ist, gilt $v_{s,max} = 2B$.

$$\Rightarrow C = 2 \cdot B \cdot H_{T_{max}}$$

4.3 Binärkanal

$X = \{x_1, x_2\}$, $Y = \{y_1, y_2\}$. Schrittfehlerwahrscheinlichkeiten: $\varepsilon := p(y_2|x_1)$, $\delta := p(y_1|x_2)$.
$\Rightarrow$ Übergangswahrscheinlichkeiten: $(p(y_j|x_i)) = \begin{pmatrix} 1-\varepsilon & \varepsilon \\ \delta & 1-\delta \end{pmatrix}$.

4.3.1 Berechnung der Transinformation

- Berechnung der $p(y_j)$
- Berechnung von $H(Y)$
- Berechnung von $H(Y|X)$
- $H_T = H(Y) - H(Y|X)$

Spezialfall symmetrisch gestört: $\varepsilon = \delta = p_s$
$H_T = H(Y) + (1-p_s) \operatorname{ld}(1-p_s) + p_s \operatorname{ld} p_s$
$H_{T,max} = 1 + (1-p_s) \operatorname{ld}(1-p_s) + p_s \operatorname{ld} p_s$ (für $p(x_1) = p(x_2) = \frac{1}{2} \Rightarrow p(y_1) = p(y_2) = \frac{1}{2}$)

Spezialfall einseitig gestört: $\varepsilon = p_s$, $\delta = 0$
$H_T = H(Y) + p(x_1)[(1-p_s) \operatorname{ld}(1-p_s) + p_s \operatorname{ld} p_s]$.
Wenn $p(x_1) = p(x_2) = \frac{1}{2} \quad \Rightarrow \quad H_T = 1 - \frac{1}{2}[(1+p_s) \operatorname{ld}(1+p_s) - p_s \operatorname{ld} p_s]$

4.4 Analoge Kanäle

Größen: P_x (mittlere Nutzsignalleistung), P_z (mittlere Störsignalleistung), P_y (mittlere Ausgangsleistung)

Voraussetzungen:

- Das Übertragungssystem enthält nur lineare Komponenten. $\Rightarrow$ Signale und Störungen überlagern sich additiv, Störungen hängen nicht vom Nutzsignal ab

- Nutz– und Störsignal sind unkorreliert. $\Rightarrow \quad P_y = P_x + P_z$
- Nutz– und Störsignal sind bandbegrenzt.

Wenn die Amplitudenwerte normalverteilt sind, gilt:
$H(X) = \frac{1}{2}\,\mathrm{ld}\,(2\pi e P_X)$, $H(Y|X) = \frac{1}{2}\,\mathrm{ld}\,(2\pi e P_z)$, $H(Y) = \frac{1}{2}\,\mathrm{ld}\,(2\pi e(P_x + P_z))$.
$H_T = H(Y) - H(Y|X) = \frac{1}{2}\,\mathrm{ld}\,(1 + \frac{P_x}{P_z})$
$C = B\,\mathrm{ld}\,(1 + \frac{P_x}{P_z})$
Rauschabstand (Signal–Stör–Verhältnis): $r = 10\,\mathrm{lg}\,\frac{P_x}{P_z} \quad [r] = \mathrm{dB}$
$\Rightarrow$ Wenn $\frac{P_x}{P_z} \gg 1$: $\quad H_T \approx 0,166\,r \qquad C \approx 0,332\,B\,r$

5 Quantisierung diskreter Signale

5.1 Zeitquantisierung

Abtasttheorem: Eine Zeitfunktion, deren Spektrum nur Komponenten im Bereich von 0 bis f_g enthält, ist vollständig bestimmt, wenn die Funktionswerte zu diskreten Zeitpunkten bekannt sind und für deren Abstand t_a gilt: $t_a \leq \frac{1}{2f_g}$, bzw. $f_a \geq 2f_g$. Dann gilt:

$$f(t) = \sum_{n=-\infty}^{+\infty} f(nt_a)\mathrm{sinc}\left(\frac{t - nt_a}{t_a}\right) \qquad \mathrm{sinc}(x) = \frac{\sin(\pi x)}{\pi x}$$

$\mathrm{sinc}(x)$ ist die Stoßantwort eines idealen Tiefpaßfilters.
$\Rightarrow$ Zeitquantisierung bringt unter dieser Bedingung ($f_A \geq 2f_g$) *keinen* Informationsverlust!

5.2 Amplitudenquantisierung

Quantisierung in m unterschiedliche Amplitudenbereiche (durch Quantisierungskennlinie).

5.2.1 Rauschabstand

Der Gleichanteil der Ausgangsleistung P_{x-} liefert keine Information und kein Rauschen. Der Rauschabstand hängt deshalb vom Schwingungsanteil $P_{x\sim}$ ab:
$\frac{P_{x\sim}}{P_z} = m^2 - 1 \quad \Rightarrow \quad r = 10\,\mathrm{lg}(m^2 - 1) \approx 20\,\mathrm{lg}\,m$

5.2.2 Quantisierung eines gestörten Signals

Welche Anzahl von Quantisierungsstufen ist sinnvoll, um die Information eines gestörten analogen Signals vollständig zu erfassen?

Für $P_z \ll P_x$ gilt: $m = \sqrt{\frac{P_x}{P_z}} = 10^{\frac{r}{20}}$.

6 Allgemeines zur Kanalkodierung

6.1 Alphabete

U	Kanalalphabet ($U = \{0, 1\}$ beim Binärkanal)
$A^* = \{a_1^*, a_2^*, \ldots, a_L^*\}$	Alphabet des Quellenkodierers; $L = \|U\|^l$
$a_i^* = (u_{i1}u_{i2}\ldots u_{il})$	i-tes Quellenkodewort
$k = n - l$	Anzahl der durch den Kanalkodierer hinzugefügten Stellen
$A = \{a_1, a_2, \ldots, a_L\}$	Alphabet des Kanalkodierers
$a_i = (u_{i1}u_{i2}\ldots u_{in})$	i-tes Kanalkodewort
$B = \{a_1, a_2, \ldots, a_{2^n}\}$	Kanalkodewort-Alphabet auf der Empfängerseite; $\|B\| > \|A\|$, da Zeichen verfälscht werden können
$B^* = A^*$	Alphabet nach korrigierender Kanaldekodierung

6.2 Hamming–Distanz

$$d_{ij} = d(a_i, a_j) = \Big|\{g \in \{1, 2, \ldots, n\} | u_{ig} \neq u_{jg}\}\Big|$$

Die HAMMING–Distanz ist die Anzahl der Stellen, in denen sich zwei Kodewörter a_i und a_j unterscheiden.

Für einen Binärkode gilt: $d_{ij} = \sum_{g=1}^{n} (u_{ig} \oplus u_{jg})$

Für die Erkenn– und Korrigierbarkeit von Fehlern interessiert besonders die minimale HAMMING–Distanz d_{min}.

Zur sicheren Erkennung von höchstens f_e Fehlerstellen ist also $d_{min} = f_e + 1$ erforderlich, zur Rekonstruktion von f_k ist $d_{min} = 2f_k + 1$ (durch Zuordnung zum Kodewort mit geringstem Abstand).

6.3 Hamming–Schranke

Die HAMMING-Schranke ist die minimale Anzahl k redundanter Stellen zur Gewährleistung der Korrektur von höchstens f_k Fehlern.

Bei Kenntnis von l und d_{min} läßt sich k folgendermaßen berechnen:

$$2^k \geq \sum_{i=0}^{\left\lfloor \frac{d_{min}-1}{2} \right\rfloor} \binom{l+k}{i}$$

Kombinationen von d_{min}, k und l, für die das Gleichheitszeichen gilt, heißen **dichtgepackt** oder **perfekt**, d. h. es befinden sich keine Binärfolgen zwischen den Korrekturkugeln und die Korrekturkugeln überschneiden sich nicht (Redundanz des Kanalkodes wird voll ausgenutzt).

6.4 Sonstige Begriffe

Ein n-stelliger Kanalkode mit k Kontrollstellen wird als $(n, n-k)$-Kode bezeichnet.

relative Redundanz: $r_k = \dfrac{k}{n}$

Koderate: $R = 1 - r_k = \dfrac{l}{n}$.

7 Lineare Blockkodes

Ein Kode heißt **linearer Blockkode** (oder **Linearkode**, **Gruppenkode**), wenn der Kanalkodierer für die Transformation der Quell– in Kanalkodewörter nur Operationen der algebraischen Struktur einer Gruppe verwendet.

Damit sind $f_e = d_{min} - 1$ Fehlerstellen erkennbar und $f_k = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ Fehlerstellen korrigierbar.

Für ein binäres Kanalalphabet wird ein Untervektorraum von $(GF(2)^n, \oplus)$ verwendet.

Dann ist die Transformation von Quell– zu Kanalkodezeichen eindeutig durch eine lineare Abbildung, d. h. deren **Generatormatrix** G der Dimension l mit l linear unabhängigen Kanalkodewörtern (Basis des Vektorraums) bestimmt.

Eine solche Generatormatrix läßt sich leicht in **kanonischer** Form durch Konkatenation der Einheitsmatrix I_l (Matrix über den Informationsstellen) und einer $l \times k$–Matrix C (Matrix über den Kontrollstellen) darstellen:

$$G = I_l C = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & c_{11} & c_{12} & \cdots & c_{1k} \\ 0 & 1 & 0 & \cdots & 0 & c_{21} & c_{22} & \cdots & c_{2k} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & c_{l1} & c_{l2} & \cdots & c_{lk} \end{pmatrix}$$

Damit ist $a_i = a_i^* \cdot G$.

Ein Linearkode heißt **systematischer** Kode, wenn einem Kanalkodewort durch Streichen der redundanten Stellen das Quellenkodewort unmittelbar entnommen werden kann.

7.1 Kontrollmatrix

Für große l ist es praktischer, anstatt der Generatormatrix G die Kontrollmatrix H zu betrachten, deren Vektoren einen Unterraum aufspannen, der zu dem von G aufgespannten Unterraum orthogonal ist:

$$G = I_l C \quad \Leftrightarrow \quad H = (-)C^T I_k$$

(Das Minus entfällt bei binären Linearkodes).

Aus H lassen sich die Kontrollelemente direkt aus den Kodeelementen berechnen.

Wegen der Orthogonalität muß das Produkt von H mit jedem Kanalkodewort 0 ergeben: Bei Verfälschungen, ergibt sich ein von 0 verschiedener Vektor (sog. **Fehlersyndrom**). Bei der Verfälschung von nur einer Stelle ist die Position des Fehlersyndroms in der Kontrollmatrix gleich der Position des verfälschten Bits.

7.2 Hamming–Kode

Dichtgepackt, 1–Fehler–korrigierend, $d_{min} = 3$, $n = 2^k - 1$.

Durch geschickte Vertauschung der Spalten in H steht in der i–ten Spalte die Binärdarstellung von i und die Kontrollstellen stehen an Positionen mit ganzen Zweierpotenzen:

$$H = \begin{array}{c} \begin{matrix} n_7 & n_6 & n_5 & n_4 & n_3 & n_2 & n_1 \end{matrix} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \\ \begin{matrix} l_4 & l_3 & l_2 & k_3 & l_1 & k_2 & k_1 \end{matrix} \end{array}$$

8 Zyklische Kodes

8.1 Definition

Ein Kode heißt **zyklisch**, wenn für jedes Kanalkodewort durch zyklische Verschiebung der Elemente (Rotation) wieder ein Kanalkodewort entsteht. Er ist ein spezieller Linearkode, der auch Körperaxiome erfüllt.

Er wird durch das **Generatorpolynom** $g(x)$ (ein Produkt irreduzibler Minimalpolynome $m_i(x)$) erzeugt und vollständig beschrieben.

8.2 Grundlagen

8.2.1 Modularpolynom

Ein **Modularpolynom** $M(x)$ ist ein irreduzibles (d. h. nicht in ein Produkt von Polynomen zerlegbares) Polynom über $GF(2)$. Es legt die Kodewortlänge n fest, die der Periode p des Zyklus der Polynomreste entspricht: $x^i \equiv x^{i+p} \bmod M(x)$. Dabei kann p maximal den Wert $p_{max} = 2^{\text{grad } M(x)} - 1$ annehmen und es gilt: $n = p$.

Gilt $p = p_{max}$, d. h., ist die Zyklusperiode der Polynomreste maximal, heißt $M(x)$ **primitiv**.

$x^{p_{max}} \bmod M(x)$ liefert bei irreduziblen Polynomen immer den Rest 1 und es gilt außerdem $n|p_{max}$. Es reicht somit, die Polynomreste nur für Teiler von p zu berechnen; ergibt sich als Rest 1, ist n durch den Wert des Exponenten bestimmt. $\Rightarrow$ Ist p_{max} prim, dann ist das irreduzible Polynom immer primitiv.

8.2.2 Erweiterungskörper, Minimalpolynom

Da ein irreduzibles Polynom $P(x)$ über $GF(q)$ mit $q \in \mathbb{P}$ keine Nullstellen in $GF(q)$ hat, diese jedoch für die Konstruktion und Dekodierung gebraucht werden, muß der Grundkörper um diese Nullstellen erweitert werden. Nach dem Fundamentalsatz der Algebra gilt:

$$P(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_{\text{grad } P(x)})$$

Ein irreduzibles Polynom $M(x)$ vom Grad k mit dem Element α als Nullstelle erzeugt einen Erweiterungskörper $GF(2^k)$, der das Nullelement und alle Potenzen $\alpha^i \quad (i = 0, 1, \dots, (2^k - 2))$ enthält. Der Zyklus der Polynomreste (mod $M(x)$) im $GF(2^k)$ bestimmt die Ordnung p des Elements α.

Jedem Element des Erweiterungskörpers ist ein **Minimalpolynom** zugeordnet, welches dem Produkt aller zu α^i konjugierten Elemente entspricht:

$$m_i(x) = (x - \alpha^{2^0 i})(x - \alpha^{2^1 i}) \dots (x - \alpha^{2^{r-1} i \bmod p})$$

r ist die Länge des Zyklus der konjugierten Elemente ($r \leq k$) und bestimmt die Anzahl der Nullstellen und den Grad von $m_i(x)$. Durch Ausmultiplizieren und Ersetzen der Potenzen von α durch die Polynomreste $\bmod M(\alpha)$ erhält man $m_i(x)$.

8.3 Generatorpolynome

8.3.1 BCH-Kodes

$g(x) = \text{kgV}\{m_\mu(x), m_{\mu+1}(x), \dots, m_{\mu+d_{min}-2}(x)\}$

μ ist eine beliebige Zahl (bei BCH–Kodes meist 0 oder 1) und parametrisiert die Leistungsfähigkeit des Kodes.

8.3.2 Zyklischer Hamming–Kode

$\mu = 1 \quad \rightarrow \quad g(x) = \text{kgV}\{m_1(x), m_2(x)\}; \quad m_1 = m_2$
$g(x) = m_1(x) = M(x) \quad \rightarrow \quad d_{min} = 3.$

8.3.3 Abramson–Kode

$g(x) = m_1(x)(x+1) \quad \rightarrow \quad d_{min} = 4.$

8.4 Kodierung und Dekodierung

Die Elemente der Kodewörter werden als Koeffizienten eines Polynoms dargestellt. Ein Kodepolynom $a(x)$ hat dann höchstens den Grad $n-1$, das Generatorpolynom den Grad k und deshalb das zu kodierende Polynom $a^*(x)$ höchstens Grad $(l-1)$, $l = n-k$.

Alle Verfahren erzeugen die gleichen Kodewörter, nur die Zuordnungen sind verschieden.

8.4.1 Generatormatrix

Zyklische Kodes als spezielle Linearkodes haben eine Generatormatrix G. Dabei nutzt man die zyklische Eingenschaft dieser Kodeklasse. Die zyklische Verschiebung um eine Stelle bedeuted Multiplikation mit x und $x^n := x^0$.

Auf Grundlage des Generatorpolynoms $g(x) = \sum_{i=0}^{k} u_i x^i$ ergibt sich $G \in \mathcal{M}((n-k) \times n, GF(2))$:

$$G = \begin{pmatrix} 0 & \cdots & 0 & 0 & u_k & \cdots & u_1 & u_0 \\ 0 & \cdots & 0 & u_k & \cdots & u_1 & u_0 & 0 \\ \vdots & \ddots & \vdots & \ldots & \ldots & \ldots & \ldots & \ldots \\ u_k & \cdots & u_1 & u_0 & 0 & \ldots & \ldots & 0 \end{pmatrix}$$

8.4.2 Multiplikationsverfahren

$a(x) = a^*(x)g(x)$

Erzeugt keinen systematischen Kode!

8.4.3 Divisionsverfahren

Die Division $\frac{a^*(x)x^k}{g(x)}$ liefert einen Rest $r(x)$. Dann ist $a(x) = a^*(x)x^k - r(x)$ (die Subtraktion ist im $GF(2)$ identisch mit der Addition).

$a^*(x)$ wird also um k Stellen nach links verschoben und $r(x)$ angehängt. Es wird somit ein systematischer Kode erzeugt.

8.5 Fehlererkennung

Alle Kodewörter (d. h. deren Polynome) sind durch $g(x)$ teilbar. Diese Eigenschaft muß für ein empfangenes Kanalwort zur Fehlererkennung überprüft werden. Ergibt sich ein Rest, so liegt eine Verfälschung vor.

Zyklische Kodes erkennen Fehlerbündel mit einer maximaler Länge grad $g(x)$.

9 Bewertung von Kanalkodes

Die relative Redundanz r_k sollte so groß wie nötig und so klein wie möglich gehalten werden. d_{min} sollte entsprechend den Fehlerwahrscheinlichkeiten angepaßt werden (alle Fehlermuster mit dem Gewicht $w(e_i) < d_{min}$ werden ja mit Sicherheit erkannt).

9.1 Größen

Blockfehlerwahrscheinlichkeit: $p_B(n) = \frac{\text{Anzahl der fehlerhaft übertragenen Blöcke}}{\text{Anzahl der insgesamt übertragenen Blöcke}}$

Restfehlerwahrscheinlichkeit: $p_R(n) = \frac{\text{Anzahl der akzeptierten falschen Blöcke}}{\text{Anzahl der insgesamt übertragenen Blöcke}}$

Reduktionsfaktor: $R_{erk} = \frac{p_R(n)}{p_B(n)} = \frac{\text{Anzahl der akzeptierten falschen Blöcke}}{\text{Anzahl der fehlerhaft übertragenen Blöcke}}$ gibt an, um welchen Faktor die Blockfehlerwahrscheinlichkeit bei der Dekodierung mit Fehlererkennung reduziert wird.

$R_{erk,max} = \frac{2^l-1}{2^n-1} \approx 2^{-k}$: ungünstigster Fall ($p_s = 0,5$, womit keine Informationsübertragung mehr möglich ist, und alle Fehlermuster gleichwahrscheinlich). Kann für Abschätzung von k verwendet werden.

9.2 Modellbetrachtung

Um quantitative Aussagen über Erkenn– und Korrigierbarkeit machen zu können, verwendet man oft das Modell eines symmetrisch gestörten Binärkanals (SBK) mit Schrittfehlerwahrscheinlichkeit p_s mit unkorellierter und binomial verteilten fehlerhaften Elementen.

Wahrscheinlichkeit, dass w Elemente verfälscht worden sind:

$$p(e_w) = \binom{n}{w} (p_s)^w (1-p_s)^{n-w}$$

Blockfehlerwahrscheinlichkeit ergibt sich aus der Summe aller Fehlermusterwahrscheinlichkeiten.

$$p_B(n) = \sum_{w=1}^{n} p(e_w) = 1 - (1-p_s)^n \approx np_s$$

$$p_R(n) = \sum_{w=1}^{n} p(e_w) R_{erk}(w)$$

$R_{erk}(w)$ ist der Anteil der Fehlermuster, die einem Kanalkodewort $a(w)$ mit dem Gewicht w entsprechen. $\Rightarrow$ $R_{erk}(w) = \frac{\text{card } a(w)}{\binom{n}{w}}$. card $a(w)$ ist dabei die Anzahl der Kanalkodewörter mit dem Gewicht w. Weil es (bis auf das Nullwort) kein Kanalkodewort mit dem Gewicht $w < d_{min}$ gibt, ist $R_{erk}(w < d_{min}) = 0$. Daher ist (in obigem Modell)

$$p_R(n) = \sum_{w=d_{min}}^{n} (p_s)^w (1-p_s)^{n-w} \text{card } a(w) \approx 2^{-k} \sum_{w=d_{min}}^{n} p(e_w) = 2^{-k} \left(1 - \sum_{w=0}^{d_{min}-1} p(e_w)\right)$$