

# 1 Wahrscheinlichkeitsrechnung

## 1.1 Begriffe

Bei **a-priori** sind die Wahrscheinlichkeiten bereits vor dem ersten Durchführen des Experimentes bekannt. Es kann auch erzwungen werden. Beispiel: Fairer Würfel. Bei **a-posteriori** werden die Wahrscheinlichkeiten ermittelt, indem das Experiment durchgeführt wird.

Wenn 2 Ereignisse **Unabhängig** sind, so verändert das Auftreten eines Ereignis nicht die Wahrscheinlichkeit des anderen Ereignis:  $P(B|A) = P(B)$ .

Ein **Elementarereignis** ist ein Ereignisraum mit nur einem Ereignis.

## 1.2 Definition Zufallsexperiment

$S$	Ereignisraum ( $\Omega$ )	$\bar{A} = S \setminus A$	Komplementärereignis
$n$	Anzahl Ereignisse in $S$	$C = A \cup B$	Ereignisse in A <b>und</b> B
$\lambda_k$	Ereignis	$C = A \cap B$	Ereignisse in A <b>oder</b> B
$A \in S$	Teilmenge von $S$	$C = S$	Sichereres Ereignis
$F_X(x)$	Verteilungsfunktion	$C = \emptyset$	Unmögliches Ereignis
$f_X(x)$	W'keitsdichte-Funktion	$B \subset A$	B ist Teil von A
$\mu_X$	Erwartungswert	$A \cap B = \emptyset$	A und B sind <b>disjunkte</b>
$\sigma_X^2$	Varianz		

## 1.3 Wahrscheinlichkeiten

$$0 \leq P(A) \leq 1 \quad P(S) = 1 \quad P(\emptyset) = 0$$

$$P(\bar{A}) = 1 - P(A)$$

$$P(B) \leq P(A) \quad \text{für } B \subset A$$

$$P(A \cup B) = P(A) + P(B) \quad \text{für disjunkte A und B}$$

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

$$P(B|A) = \frac{P(A \cap B)}{P(A)} = P(A|B) \cdot \frac{P(B)}{P(A)}$$

$$P(A \cap B) = P(A) \cdot P(B) \quad \text{wenn A und B Unabhängig}$$

## 1.4 Verteilungsfunktion

$$F_X(x) = P(X \leq x) \quad \text{für } x \in (-\infty, \infty), \quad F_X(-\infty) = 0 \quad F_X(\infty) = 1$$

$$P(a < x \leq b) = F_X(b) - F_X(a) \quad P(X > a) = 1 - F_X(a)$$

$$f_X(x) = \frac{dF_X(x)}{dx} \geq 0 \quad F_X(x) = \int_{-\infty}^x f_X(\tilde{x}) \cdot d\tilde{x} \quad \int_{-\infty}^{\infty} f_X(x) \cdot dx = 1$$

## 1.5 Mehrdimensionale Zufallsvariablen

$$F_{XY}(x, y) \quad \text{W'keit von 2 ZV}$$

$$p_{XY}(x, y) \quad \text{Verbundsw'keitsf.}$$

$$Z = g(X, Y) \quad \text{Kombinierte ZV}$$

$$F_{XY}(x, y) = P(X \leq x, Y \leq y)$$

$$p_{XY}(x, y) = P(X = x_i, Y = y_k)$$

(1) Wenn statistisch Unabhängig:

$$F_{XY}(x, y) = F_X(x) \cdot F_Y(y)$$

$$p_{XY}(x, y) = p_X(x) \cdot p_Y(y)$$

Randverteilungsfunktion:

$$F_X(x) = F_{XY}(x, +\infty)$$

$$F_Y(y) = F_{XY}(+\infty, y)$$

Verbundsw'keitsfunktion

$$p_X(x) = \sum_{y_k} p_{XY}(x, y_k)$$

$$p_Y(y) = \sum_{x_i} p_{XY}(x_i, y)$$

### 1.5.1 Verbundw'keitsdichtefunktion

$$f_{XY}(x, y) = \frac{\partial^2 F_{XY}(x, y)}{\partial x \cdot \partial y} = f_X(x) \cdot f_Y(y) \quad \text{falls X, Y statistisch Unabhängig}$$

$$f_X(x) = \int_{-\infty}^{\infty} f_{XY}(x, y) dy \quad f_Y(y) = \int_{-\infty}^{\infty} f_{XY}(x, y) dx$$

### 1.5.2 Erwartungswert (n-tes Moment) & Varianz

$$\mu_X = E[X] = \sum_i x_i \cdot p_X(x_i) = \int_{-\infty}^{\infty} x \cdot f_X(x) \cdot dx = \text{"Wert" \cdot W'keit}$$

$$\text{Linearität des Erwartungswert} \quad E[X + Y] = E[X] + E[Y]$$

$$E(cX) = cE[X]$$

**Erwartungswert & Moment**

$$E[Y] = E[g(X)] = \sum_i g(x_i) \cdot p_X(x_i) = \int_{-\infty}^{\infty} g(x) \cdot f_X(x) \cdot dx$$

$$E[Z] = E[g(X, Y)] = \sum_i \left( \sum_j g(x_i, y_j) \cdot p_{XY}(x_i, y_j) \right)$$

$$E[Z] = E[g(X, Y)] = \int_{-\infty}^{\infty} \left( \int_{-\infty}^{\infty} g(x, y) \cdot f_{XY}(x, y) dx \right) dy$$

$$\text{n-tes Moment: } E(X^n) = \sum_i x_i^n \cdot p_X(x_i) = \int_{-\infty}^{\infty} x^n \cdot f_X(x) \cdot dx$$

**Varianz**

$$\sigma_X^2 = \text{Var}(X) = E[X^2] - \mu_X^2 = \sum_i (x_i - \mu_X)^2 \cdot p_X(x_i)$$

$$\sigma_X^2 = \text{Var}(X) = \int_{-\infty}^{\infty} (x - \mu_X)^2 \cdot f_X(x) \cdot dx$$

**1.5.3 (k,n)-tes Moment  $m_{kn}$ , Korrelation  $m_{11}$** 

$$m_{kn} = E[X^k Y^n] = \sum_j \left( \sum_i x_i^k y_j^n \cdot p_{XY}(x_i, y_j) \right)$$

$$m_{kn} = E[X^k Y^n] = \int_{-\infty}^{\infty} \left( \int_{-\infty}^{\infty} x^k y^n \cdot f_{XY}(x, y) \cdot dx \right) dy$$

$$\text{Spezialfall: Korrelation } m_{11} = E[XY]$$

**1.5.4 Kovarianz  $\sigma_{XY}$** 

$$\sigma_{XY} = \text{Cov}(X, Y) = E[(X - \mu_X) \cdot (Y - \mu_Y)]$$

$$\sigma_{XY} = E[XY] - E[X] \cdot E[Y] = m_{11} - \mu_X \cdot \mu_Y$$

Die zwei Zufallsvariablen  $X$  und  $Y$  sind **unkorreliert**, falls  $\sigma_{XY} = 0$ . Statistisch unabhängige Zufallsvariablen sind unkorreliert.

**1.5.5 Korrelations-Koeffizient  $\rho(PX)$** 

$$\rho(X, Y) = \rho_{XY} = \frac{\sigma_{XY}}{\sigma_X \cdot \sigma_Y} \quad |\rho_{XY}| \leq 1$$

**1.6 Verteilungen**

$$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!} \quad (\text{TR: ncr})$$

**1.6.1 Binomialverteilung**

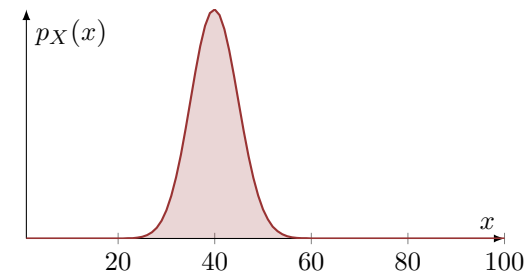
Ein Experiment mit 2 möglichen Ausgängen, welche mit der W'keit  $p$ , bzw.  $1-p$  zutreffen, wird  $n$  mal wiederholt. Die ZV  $x$  ist die Anzahl, wie oft ein Ausgang eintritt.

$$\mu_X = n \cdot p \quad \sigma_X^2 = np \cdot (1-p)$$

$$p_X(k) = \binom{n}{k} p^k \cdot q^{n-k}$$

$$F_X(x) = \sum_{k=0}^m \binom{n}{k} p^k \cdot q^{n-k}$$

**Grafik:**  $p = 0.4, n = 100$

**1.6.2 Poissonverteilung**

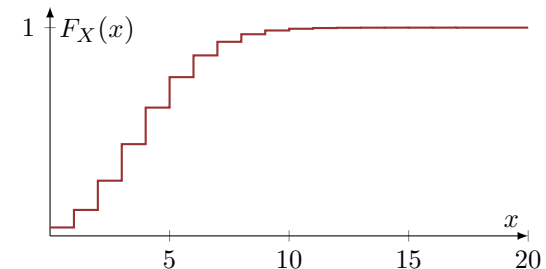
Eintreten eines seltenen Ereignis ( $p \ll 1$ ) innerhalb einer gewissen Zeitspanne. In NaT wird es jedoch meistens in einer gewissen Länge  $n$  betrachtet.

$$\mu_X = np = \lambda \quad \sigma_X^2 = np = \lambda$$

$$p_X(k) = e^{-\lambda} \cdot \frac{\lambda^k}{k!}$$

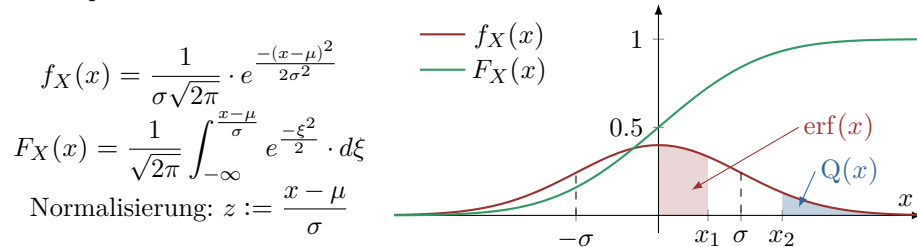
$$F_X(x) = e^{-\lambda} \cdot \sum_{k=0}^x \frac{\lambda^k}{k!}$$

**Grafik:**  $n = 1000, p = 0.005$



### 1.6.3 Normalverteilung (Gaussverteilung)

Anwendbar bei einer ZV, welche aus vielen Faktoren besteht. Beispiel: thermische Rauschquelle.



$$f_X(x) = \frac{1}{\sigma\sqrt{2\pi}} \cdot e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

$$F_X(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{x-\mu}{\sigma}} e^{-\frac{\xi^2}{2}} \cdot d\xi$$

Normalisierung:  $z := \frac{x-\mu}{\sigma}$

$Q(z)$  als Skalierung

$$Q(z) = \frac{1}{\sqrt{2\pi}} \int_z^{\infty} e^{-\frac{\xi^2}{2}} d\xi$$

$$F_X(x) = 1 - Q\left(\frac{x-\mu}{\sigma}\right) = 1 - Q(z)$$

$$Q(-z) = -Q(z)$$

$\text{erf}(x)$  als Matlab-Funktion:

$$\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-\xi^2} d\xi$$

$$F_X(x) = \frac{1}{2} \left( 1 + \text{erf}\left(\frac{x-\mu}{\sqrt{2}\sigma}\right) \right)$$

## 2 Zufallsprozesse

$X(t, \lambda)$  Zufallsprozess

$X(t, \lambda_i) = x_i(t)$  Musterfunktion

$X_k(\lambda)$  ZV zum Zeitpunkt  $t_k$

$F_{X_k}(x_k; t_k)$  Verteilungsfunktion

$f_{X_k}(x_k; t_k)$  W'keitsdichtefunktion

$\mu_X(t)$  Erwartungswert von  $X(t)$

$R_{XX}(t_1, t_2)$  Autokorrelation

$C_{XX}(t_1, t_2)$  Autokovarianz

$C_{XX}(t_1, t_2) = 0$  ZV sind unkorreliert

$$F_{X_k}(x_k; t_k) = P\{X_k(t_k) \leq x_k\}$$

$$f_{X_k}(x_k; t_k) = \frac{\partial F_{X_k}(x_k; t_k)}{\partial x_k}$$

$$F_X(x_1, x_2; t_1, t_2)$$

$$= P\{X(t_1) \leq x_1, X(t_2) \leq x_2\}$$

$$f_X(x_1, x_2; t_1, t_2) = \frac{\partial^2 F_X(x_1, x_2; t_1, t_2)}{\partial x_1 \partial x_2}$$

$$\tau = t_1 - t_2$$

### 2.1 Statische Kennwerte

$$\mu_x(t) = E[X(t)] = \int_{-\infty}^{+\infty} x \cdot f_X(x; t) dx$$

$$R_{XX}(t_1, t_2) = E[X(t_1)X(t_2)] = \iint_{-\infty}^{+\infty} x_1 x_2 \cdot f_X(x_1, x_2; t_1, t_2) \cdot dx_1 \cdot dx_2$$

$$C_{XX}(t_1, t_2) = R_{XX}(t_1, t_2) - \mu_x(t_1) \cdot \mu_x(t_2)$$

### 2.2 Stationarität

Ein Zufallsprozess ist Stationär, wenn ihre statistischen Eigenschaften zeitlich unverändert bleiben. Man unterscheidet streng und schwach stationäre Prozesse.

#### 2.2.1 Statische Eigenschaften

$$\bar{x} = \langle x(t) \rangle = \lim_{T \rightarrow \infty} \frac{1}{T} \int_{-T/2}^{T/2} x(t) dt$$

$$\overline{R_{XX}}(\tau) = \langle x(t) \cdot x(t+\tau) \rangle = \lim_{T \rightarrow \infty} \frac{1}{T} \int_{-T/2}^{T/2} x(t) \cdot x(t+\tau) dt$$

$$E[\bar{x}] = \lim_{T \rightarrow \infty} \frac{1}{T} \int_{-T/2}^{T/2} E[x(t)] dt = \lim_{T \rightarrow \infty} \frac{1}{T} \int_{-T/2}^{T/2} \mu_x(t) dt$$

#### 2.2.2 Streng stationärer Zufallsprozess (SSS)

Alle statischen Eigenschaften eines SSS-Prozesses sind unabhängig von einer beliebigen Zeitverschiebung  $t_c$ :

$$E[X(t)] = \mu_x$$

$$R_{XX}(t_1, t_2) = R_X(\tau)$$

$$C_{XX}(t_1, t_2) = R_X(\tau) - \mu_x^2$$

#### 2.2.3 Schwach stationärer Zufallsprozess (WSS)

Ein Zufallsprozess ist schwach stationär, sobald folgende Eigenschaft erfüllt ist:

$$f_X(x_1, x_2; t_1, t_2) = f_X(x_1, x_2; t_1 + t_c, t_2 + t_c)$$

$$E[X(t)] = \mu_x$$

$$R_{XX}(t_1, t_2) = R_X(\tau)$$

$$C_{XX}(t_1, t_2) = R_X(\tau) - \mu_x^2 = C_{XX}(\tau)$$

### 2.2.4 Ergodizität

Ein Stationärer Prozess ist ergodisch, wenn zusätzlich auch jede einzelne Musterfunktion dieselben Zeitmittelwerte besitzt, und wenn diese mit den statischen Kennwerten der Schar übereinstimmt.

$$E[X(t)] \quad \text{DC-Level}$$

$$E[X(t)]^2 \quad \text{DC-Leistung}$$

$$E[X^2(t)] \quad \text{Gesamtleistung}$$

$$\sigma_X^2(t) \quad \text{AC-Leistung}$$

$$X(t) \quad \text{RMS-Level}$$

$$\bar{x}_i = \overline{x_i(t)} = E[x(t)] = \mu_X$$

$$E[\overline{x(t)}] = \mu_X$$

$$E[X(t)] = \bar{x} = \langle x(t) \rangle$$

$$E[X(t)]^2 = \langle x(t) \rangle^2$$

$$E[X^2(t)] = R_{XX}(t) = \langle x^2(t) \rangle$$

$$\sigma_X^2(t) = \langle x^2(t) \rangle - \langle x(t) \rangle^2$$

$$\sigma_X(t) = \overline{\sigma_X}$$

### 2.2.5 Eigenschaften von stationären Zufallsprozessen

Auto- und Kreuzkorrelationsfunktion bei WSS Prozessen:

$$R_{XX}(-\tau) = R_{XX}(\tau)$$

$$R_{XX}(\tau) = E[X(t)X(t+\tau)] \quad |R_{XX}(\tau)| \leq R_{XX}(0)$$

$$R_{XX}(0) = E[X^2(x)]$$

$$R_{XY}(-\tau) = R_{XY}(\tau)$$

$$R_{XY}(\tau) = E[X(t)Y(t+\tau)] \quad |R_{XY}(\tau)| \leq \frac{1}{2} (R_{XX}(0) + R_{YY}(0))$$

$$R_{XY}(\tau) \leq \sqrt{R_{XX}(0)R_{YY}(0)}$$

Auto- und Kreuzkovarianz bei WSS Prozessen:

$$C_{XX}(\tau) = R_{XX}(\tau) - \mu_X^2$$

$$C_{XY}(\tau) = R_{XY}(\tau) - \mu_X \cdot \mu_Y$$

$$C_{XY}(\tau) = 0 \rightarrow \text{Zufallsprozesse sind zueinander unkorreliert}$$

Spektrale **Leistung** bei WSS Prozessen:

$$S_{XX}(\omega) = E \left[ \lim_{T \rightarrow \infty} \frac{1}{T} \cdot X(\omega)^2 \right] = \lim_{T \rightarrow \infty} \frac{1}{T} \cdot E[|X(\omega)|^2]$$

$$S_{XX}(\omega) = \int_{-\infty}^{+\infty} R_{XX}(\tau) \cdot e^{-j\omega\tau} d\tau \quad R_{XX}(\tau) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} S_{XX}(\omega) \cdot e^{j\omega\tau} d\omega$$

### 2.3 Übertragung von Zufallsprozessen über LTI-Systeme

$$Y(t) = X(t) * h(t) = \int_{-\infty}^{+\infty} h(u)X(t-u)du \quad \xrightarrow{X(t)} \boxed{h(t)} \xrightarrow{\quad} Y(t)$$

$$\mu_Y(t) = h(t) * \mu_X(t) \stackrel{\text{WSS}}{=} H(0) \cdot \mu_X$$

$$R_{YY}(t_1, t_2) = \iint_{-\infty}^{+\infty} h(u_1) \cdot h(u_2) \cdot R_{XX}(t_1 - u_1, t_2 - u_2) \cdot du_1 \cdot du_2$$

$$R_{YY}(\tau) \stackrel{\text{WSS}}{=} \iint_{-\infty}^{+\infty} h(u_1) \cdot h(u_2) \cdot R_{XX}(\tau + u_1 - u_2) \cdot du_1 \cdot du_2$$

Wenn  $X(t)$  ein WSS-Prozess ist, ist  $Y(t)$  auch ein WSS-Prozess.

#### 2.3.1 Leistungsdichtespektrum

$$S_{YY}(\omega) = \int_{-\infty}^{+\infty} R_{YY}(\tau) \cdot e^{-j\omega\tau} d\tau = H^*(\omega) \cdot H(\omega) \cdot S_{XX}(\omega) = |H(\omega)|^2 \cdot S_{XX}(\omega)$$

$$R_{YY}(\tau) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} |H(\omega)|^2 \cdot S_{XX}(\omega) \cdot e^{j\omega\tau} d\omega$$

$$E[Y^2(t)] = R_{YY}(0) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} |H(\omega)|^2 \cdot S_{XX}(\omega) d\omega$$

### 2.4 Spezielle Zufallsprozesse

#### 2.4.1 Gauss'scher Zufallsprozess

Zu jedem Zeitpunkt  $t_i$  ist die Zufallsvariable  $X(t_i)$  normalverteilt. Ist ein gauss'scher Zufallsprozess WSS, ist er auch SSS. Ein gauss'scher Zufallsprozess  $X(t)$  ist am Ausgang eines LTI Systems  $Y(t)$  auch gaussisch.

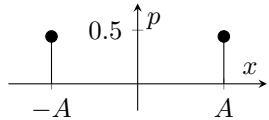
$$f_x(x_1, x_2; t_1, t_2) = \frac{1}{2\pi\sigma_{x_1}\sigma_{x_2}} \cdot e^{-\frac{(x_1 - \mu_{x_1})^2}{2\sigma_{x_1}^2}} \cdot e^{-\frac{(x_2 - \mu_{x_2})^2}{2\sigma_{x_2}^2}}$$

Wenn  $C_{XX}(t_1, t_2) = 0$ , dann ist  $f_{XX}(x_1, x_2; t_1, t_2) = f_X(x_1; t_1) \cdot f_X(x_2; t_2)$

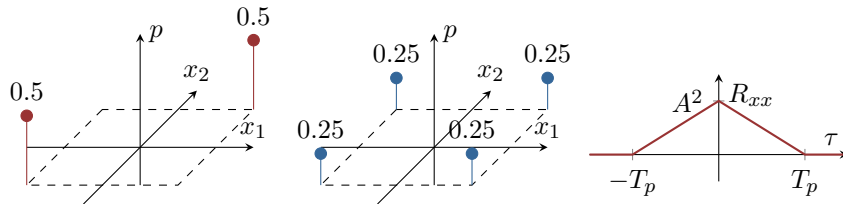
## 2.5 Spektren von Zufallssesquenzen berechnen

1. Stationärer Zufallsprozess wird vorausgesetzt: Musterfunktion darf um eine beliebige Verschiebung  $\Delta t$  verschoben werden. Zu jedem Zeitpunkt ist jede Sequenz denkbar.

2. Eindimensionale (diskrete) Amplitudenverteilung:  $p_X(x)$

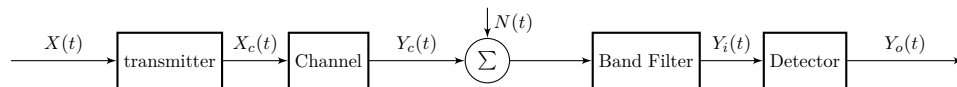


3. Zweidimensionale (diskrete) Amplitudenverteilung:  $p_{XX}(x_1, x_2)$ . **Rot:**  $\tau = 0$ , **Blau:**  $\tau > T_p$ , dazwischen linearer Anstieg. Danach muss die AFK berechnet werden:  $R_{XX}(\tau) = \sum_i \sum_j x_i \cdot x_j \cdot p_{XX}(x_i, x_j)$



4.  $\mathcal{F}(R_{XX}(\tau)) \Rightarrow S_{XX}(\omega)$

## 3 Rauschen in analogen Kommunikationssystemen:



Das Rauschsignal  $N(t)$  ist ein stationärer und ergodischer Zufallsprozess, welcher mit  $X(t)$  unkorreliert ist. Ausserdem gilt:  $E[N(t)] = 0$ ,  $E[X(t) \cdot N(t)] = 0$ . Der Frequenzgang  $S_{nn}(\omega) = \frac{\eta}{2}$ .

Das Nachrichtensignal ist ein Zufallsprozess  $X(t)$  mit  $|X(t)| \leq 1$ , bzw.  $|x_\lambda(t)| \leq 1$  für alle  $\lambda$  des Ereignisraums  $s$ . Die Leistung  $S_X = S_X(t) = E[X^2(t)] \leq 1$ . Ausserdem ist das Signal  $X(t)$  bandbeschränkt mit der Bandbreite  $B$ .

Additive white gaussian noise: AWGN

	Baseband	DSB-SC	AM
Eingangsnutzsignal $X_i(t)$	$X(t)$	$X(t) \cdot A_c \cdot \cos(\omega_c t)$	$A_c(1 + \mu X(t)) \cos(\omega_c t)$
Leistung $S_i$ von $X_i(t)$	$S_x$	$\frac{1}{2} \cdot A_c^2 \cdot S_x$	$\frac{1}{2} A_c^2 (1 + \mu^2 S_x)$
Bandbreite von $X_i(t)$	$B$	$2B$	$2B$
Leistung $S_{Ni}$ von $N_i(t)$	$\eta B$	$2\eta B$	$2\eta B$
SNR <sub>i</sub>	$\frac{S_i}{\eta B}$	$\frac{A_c^2 S_x}{4\eta B}$	$\frac{A_c^2 (1 + \mu^2 S_x)}{4\eta B}$
Ausgangsnutzsignal $X_o(t)$	$X(t)$	$A_c \cdot X(t)$	$A_c \cdot \mu \cdot X(t)$
Leistung $S_o$ von $X_o(t)$	$S_X$	$A_c^2 S_x$	$A_c^2 \cdot \mu^2 \cdot S_X$
Leistung $S_{No}$ von $N_o(t)$	$\eta B$	$2\eta B$	$2\eta B$
SNR <sub>o</sub>	$\frac{S_i}{\eta B}$	$\frac{A_c^2 S_X}{2\eta B}$	$\frac{A_c^2 \mu^2 S_X}{2\eta B}$
SNR <sub>o</sub> mit $\gamma$	$\gamma$	$\gamma$	$\frac{\mu^2 S_X}{1 + \mu^2 S_X} \cdot \gamma$
	PM		FM
Eingangsnutzsignal $X_i(t)$	$A_c \cdot \cos(\omega_c t + k_p \cdot X(t))$		$A_c \cos(\omega_c t + k_f \int_{-\infty}^t X(\tau) d\tau)$
Leistung $S_i$ von $X_i(t)$	$\frac{1}{2} A_c^2$		$\frac{1}{2} A_c^2$
Bandbreite von $X_i(t)$	$2(D+1)B$		$2(D+1)B$
Leistung $S_{Ni}$ von $N_i(t)$	$2(D+1)\eta B$		$2(D+1)\eta B$
Ausgangsnutzsignal $X_o(t)$	$\frac{A_c^2}{4(D+1)\eta B}$		$\frac{A_c^2}{4(D+1)\eta B}$
Leistung $S_o$ von $X_o(t)$	$k_p \cdot X(t)$		$k_f < c \cdot X(t)$
SNR <sub>i</sub>	$k_p^2 S_X$		$k_f^2 S_X$
Leistung $S_{No}$ von $N_o(t)$	$\frac{2}{A_c^2} \eta B$		$\frac{2(2\pi B)^2}{3A_c^2} \eta B$
SNR <sub>o</sub>	$\frac{k_p^2 A_c^2 S_x}{2\eta B}$		$\frac{3D^2 A_c^2 S_X}{2\eta B}$
SNR <sub>o</sub> mit $\gamma$	$k_p^2 \cdot S_x \cdot \gamma$		$3D^2 \cdot S_X \cdot \gamma$

### 3.1 Rauschen bei Winkelmodulierten Systemen

Bei den PM- / FM-Systemen gilt für das Hubverhältnis  $D = \frac{\Delta f}{B_m} = \frac{\delta \omega}{W_m}$

$$Y_i(t) = A_c \cos(\omega_c t + \varphi(t)) + n_i(t) \quad \text{mit} \quad S_i = \frac{1}{2} A_c^2$$

$$\varphi_{PM} = k_p \cdot X(t) \quad \varphi_{FM}(t) = k_f \int_{-\infty}^t X(\tau) d\tau$$

$$Y_{oPM}(t) = \Theta(t) = k_p X(t) + \frac{n_s(t)}{A_c} \quad Y_{oFM}(t) = \frac{d\Theta(t)}{dt} = k_f X(t) + \frac{n_s(t)}{A_c}$$

### 3.2 Additive White Gaussian Noise AWGN

Beispiel: thermisches Rauschen von Widerständen.  $S_{XX}(\omega)$ : Spektrale Leistung,  $B$ : Bandbreite des Rauschen.

$$S_{XX}(\omega) = \frac{\eta}{2}, \quad R_{XX}(\tau) = \frac{\eta}{2} \cdot \delta(\tau), \quad \eta = \frac{\sigma^2}{B}$$

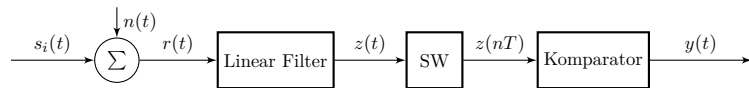
### 3.3 Farbige Rauschsignale

Pink noise:  $S_{XX}(\omega) = c \cdot \frac{1}{\omega}$  Brown noise:  $S_{XX}(\omega) = c \cdot \frac{1}{\omega^2}$

Blue noise:  $S_{XX}(\omega) = c \cdot \omega$  Purple noise:  $S_{XX}(\omega) = c \cdot \omega^2$

## 4 Optimaler Detektor

Der Empfänger soll so optimiert werden, dass er den übertragenen digitalen Datenstrom die Bitfehlerrate  $P_e$  minimiert. Also muss die Signal-Noise-Ratio klein sein. Das Rauschsignal  $n(t)$  ist ein Mittelwertfreies AWGN (additive white gaussian noise). der Abtaster erzeugt das diskrete Signal  $z(nT) = a_i(nT) + n_0(nT)$  (zu en Zeitpunkten  $nT$ ).



$$s_i(t) = \begin{cases} s_1(t) & 0 \leq t \leq T \quad \text{for binary 1} \\ s_2(t) & 0 \leq t \leq T \quad \text{for binary 0} \end{cases} \quad r(t) = s_i(t) + n(t)$$

### 4.1 Detektor

Der Detektor entscheidet durch eine Schätzung, welches Signal höchstwahrscheinlich gesendet wurde. bei Soft-Decision wird anstatt fester Entscheidung eine W'keit für die beiden Symbolwerte bestimmt und verarbeitet.

Hypothese  $H_1$  (falls  $z(nT) > \lambda$ ):  $s_1$  wurde gesendet

Hypothese  $H_1$  (falls  $z(nT) < \lambda$ ):  $s_2$  wurde gesendet

Ein Bitfehler ist, wenn das falsche Bit erkannt wird. Bei Soft-Decision bildet die W'keit ein Anhaltspunkt für mögliche Bitfehler. bei Hard-Decision kann mit folgender Fehlerw'keit gerechnet werden:

$$P_e = P(H_2|s_1) + P(H_1|s_2) \cdot P(s_2)$$

$$P_e = \frac{1}{2} [P(H_2|s_1) + p(H_1|s_2)], \quad \text{wenn: } P(s_1) = P(s_2) = \frac{1}{2}$$

### 4.2 Maximum Likelihood Detector

$z(nT)$  sei die Verteilung in Funktion von  $s_1$  und  $s_2$ .

$$\text{Hypothese } H_1 : \Lambda(z) = \frac{f(z|s_1)}{f(z|s_2)} > \frac{P(s_2)}{P(s_1)}$$

$$\text{Hypothese } H_2 : \Lambda(z) = \frac{f(z|s_1)}{f(z|s_2)} < \frac{P(s_2)}{P(s_1)}$$

Beim vereinfachten ML Detector wird vorausgesetzt, dass  $P(s_1) = P(s_2) = \frac{1}{2}$ . Somit wird  $\frac{P(s_2)}{P(s_1)} = 1$ .

### 4.3 Beispiel: verrauschtes NRZ-Signal

ein Signal  $s$  mit den beiden möglichen Werten  $s_1 = a_1, s_2 = a_2$  wird durch ein weisses Rauschen verfälscht:

$$f_{n_0}(\xi) = \frac{1}{\sqrt{2\pi}\sigma_{n_0}} \cdot e^{-\frac{\xi^2}{2\sigma_{n_0}^2}}$$

$$\Rightarrow f(z|s_1) = \frac{1}{\sqrt{2\pi}\sigma_{n_0}} \cdot e^{-\frac{(z-a_1)^2}{2\sigma_{n_0}^2}}, \quad f(z|s_2) = \frac{1}{\sqrt{2\pi}\sigma_{n_0}} \cdot e^{-\frac{(z-a_2)^2}{2\sigma_{n_0}^2}}$$

Somit ist die Wahrscheinlichkeit, dass die falsche Hypothese gewählt wird:

$$P(H_1|s_1) = \int_{-\infty}^{\lambda_0} f(z|s_1) dz, \quad P(H_1|s_1) = \int_{-\infty}^{\lambda_0} f(z|s_1) dz$$

Mit den Vereinfachungen, dass  $P(s_1) = P(s_2) = 0.5$  und  $\lambda_0 = \frac{a_1+a_2}{2}$ , dann ist die Wahrscheinlichkeit  $P_e$ , dass die falsche Hypothese gewählt wurde:

$$P_e = Q\left(\frac{a_1 - a_2}{2\sigma_{n_0}}\right)$$

## 4.4 Matched Filter

Das Lineare Filter  $H(\omega)$  soll die Fehler-WSK zum Zeitpunkt  $T$  minimieren.

$$H(\omega) = S^*(\omega) \cdot e^{-j\omega T}$$

↓

$H(\omega)$	Übertragungsfunktion des Filters	$h(t) = \begin{cases} s(T-t) & 0 \leq t \leq T \\ 0 & \text{sonst} \end{cases}$ $\left(\frac{S}{N}\right)_{\text{max}} = \frac{(a_1 - a_2)^2}{\sigma_{n_0}^2} = \frac{2E_d}{\eta}$ $E_d = \int_0^T [s_1(t) - s_2(t)]^2 dt$ $P_e = Q\left(\frac{a_1 - a_2}{2\sigma_{n_0}}\right) = Q\left(\sqrt{\frac{E_d}{2\eta}}\right)$
$s(t)$	Differenzsignal $s_1 - s_2$	
$a_1, a_2$	Signalwerte von $s_1, s_2$	
$S(\omega)$	Spektrale Leistung des Signals	
$E_d$	Energie des Differenzsignals $s(t)$	
$P_e$	Fehlerwahrscheinlichkeit	

### 4.4.1 Variante zum matched-Filter: Korrelator

zum Sample Zeitpunkt  $t = T$  ist die Antwort  $z(t)$  eines Matched Filters und diejenigen eines **Korrelators** identisch. ein Korrelator multipliziert zwei Signale  $s(t)$  und  $r(t)$  und integriert das Resultat.

$$\underbrace{z(t) = r(t) * h(t)}_{\text{Matched Filter}} = \underbrace{\int_0^t r(\tau) h(t - \tau) d\tau}_{\text{Korrelator}} = \underbrace{\int_0^t r(\tau) s(T - (t - \tau)) d\tau}_{\text{Korrelator}} \stackrel{t=T}{=} \int_0^T r(\tau) s(\tau) d\tau$$

## 5 Informationen

- **Information** (mathematische Betrachtung): Antwort auf eine konkrete Fragestellung. Die Fragen können geschickter gestellt werden, um die Anzahl der Fragen zu minimieren. Fragen sind dann geschickt gewählt, wenn bei wiederholtem Zufallsexperiment im Schnitt die Anzahl Fragen minimal ist. Bei binärer Sichtweise sind Fragen dann optimal, wenn sie **mit 50% Wahrscheinlichkeit** mit Ja oder Nein beantwortet werden. So werden wahrscheinliche Ergebnisse mit wenigen Fragen gefunden.
- **DMS**: Discrete memoryless source (jedes neue Symbol ist unabhängig von vorhergehenden Symbolen).

- **DMC**: Discrete memoryless Channel (der Ausgang  $Y_i$  ist nur abhängig von  $X_i$ , und nicht von  $X_k, k \neq i$ ).

## 5.1 Mathematische Beschreibung

$I(X_i)$	Informationsgehalt des Ereignis $X_i$	$R(X)$	Redundanz der Quelle X
$H(X)$	Entropie des Alphabets einer Quelle X	$r$	Symbolrate
$m$	Grösse des Alphabets in anz. Zeichen	$R$	Informationsrate

$$I(X_i) = -\log_2 P(X_i)$$

$$I(X_i) \geq 0$$

$$I(X_i) > I(X_k), \quad \text{wenn } P(X_i) < P(X_k)$$

$$I(X_i, X_k) = I(X_i) + I(X_k), \quad \text{wenn } X_i, X_k \text{ statistisch unabhängig}$$

$$H(X) = E[I(X_i)] = \sum_i P(X_i) \cdot I(X_i) = - \sum_i P(X_i) \cdot \log_2 P(X_i)$$

$$0 \leq H(X) \leq \log_2 m \quad \text{für binäre Quellen: } 0 \leq H(X) \leq 1$$

$$H_{\max}(X) = \log_2 m$$

$$R(X) = H_{\max}(X) - H(X) = \log_2 m + \sum_i P(X_i) \cdot \log_2 P(X_i) \quad R = r \cdot H(X)$$

## 5.2 Kanaldarstellung

Die **Kanalmatrix** gibt für jedes gesendete Symbol  $x_i$  die bedingte Wahrscheinlichkeit  $P(y_i|y_i)$  an, dass der Empfänger ein  $y_i$  dedektiert.

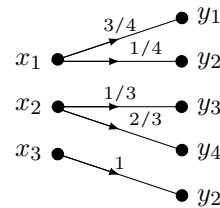
$$[P(Y|X)] = \begin{bmatrix} P(y_1|x_1) & P(y_1|x_1) & \dots & P(y_n|x_1) \\ P(y_1|x_2) & P(y_1|x_2) & \dots & P(y_n|x_2) \\ \vdots & \vdots & \ddots & \vdots \\ P(y_1|x_m) & P(y_1|x_m) & \dots & P(y_n|x_m) \end{bmatrix}$$

Die **Verbundmatrix** gibt die Wahrscheinlichkeiten von sämtlichen Kombinationen von gesendeten und empfangenen Symbolen  $X_i$  und  $Y_i$  an.

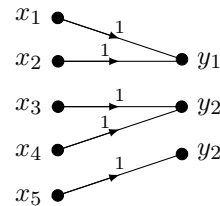
$$[P(Y, X)] = \begin{bmatrix} P(y_1, x_1) & P(y_2, x_1) & \dots & P(y_n, x_1) \\ P(y_1, x_2) & P(y_2, x_2) & \dots & P(y_n, x_2) \\ \vdots & \vdots & \ddots & \vdots \\ P(y_1, x_m) & P(y_2, x_m) & \dots & P(y_n, x_m) \end{bmatrix}$$

**Verlustloser Kanal:**

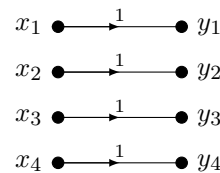
$$[P(Y|X)] = \begin{bmatrix} \frac{3}{4} & \frac{1}{4} & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & \frac{2}{3} & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

**Deterministischer Kanal:**

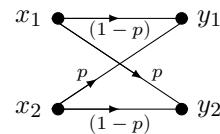
$$[P(Y|X)] = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

**Rauschfreier Kanal:**

$$[P(Y|X)] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

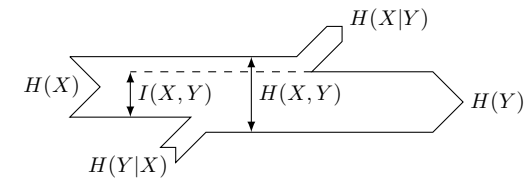
**Binärer symmetrischer Kanal:**

$$[P(Y|X)] = \begin{bmatrix} (1-p) & p \\ p & (1-p) \end{bmatrix}$$



### 5.3 Bedingte Entropie

- $H(Y|X)$  ist der Informationsbedarf, um aus gesendetem  $X$  das empfangene  $Y$  zu bestimmen.
- $H(X|Y)$  ist der Informationsbedarf um aus empfangenem  $Y$  das gesendete  $X$  zu bestimmen. (Information aus dem Empfänger, welche notwendig ist, um zu wissen, was gesendet wurde.)
- $H(X, Y)$ : die Verbundentropie ist die Information des gesamten Kommunikationskanals. Das ist der Informationsgehalt der gesendeten und Empfangenen Symbole, sowie deren Beziehung zueinander.
- $I(X, Y)$  ist die Information, welche vom Eingang zum Ausgang des Kanals transferiert wird.



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

$$I(X, Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(Y, X)$$

$$I(X, Y) = H(X) + H(Y) - H(X, Y)$$

### 5.4 Kanalkapazität

Die Kanalkapazität  $C_s$ ,  $C$  ist die W'keitsverteilung von  $X$ , welche den Informationsfluss über den Kanal maximiert. Dabei ist da Eingangs- und Ausgangsalphabet, sowie die Kanalmatrix  $P(Y|X)$  gegeben. Hier ist  $r$ : Symbolrate

$$C = r \cdot C_s = r \cdot \max I(X, Y)$$



## 6 Quellenkodierung

- **Fixed Length Code:** Jedes Codewort hat die gleiche Länge (Bsp: ASCII-Code)
- **Variable Length Code:** Je nach Häufigkeit wird die Länge der Codewörter bestimmt (Bsp: Morse, Shannon-Fano, Huffman)
- **Prefix-Free Code:** Kein Codewort ist Präfix eines anderen Codeworts (Bsp: Shannon-Fano, Huffman)
- **Uniquely Decodable Code:** Eine Kette von Codewörtern kann eindeutig wieder in die ursprüngliche Symbolfolge zurückgewandelt werden.
- **Instantaneous Code:** Eindeutig decodierbarer Code, welcher nach dem Empfangen jedes einzelnen Codeworts sofort ein eindeutiges Symbol liefert, ohne dass nachfolgende Symbole decodiert werden müssen.

### 6.1 Optimaler Code

Jeder Instantaneous Code, welcher eine minimale Codelänge besitzt, ist ein optimaler Code.

$L$	Mittlere Codelänge	$L = \sum_i P(x_i) \cdot n_i \geq H(X)$
$\eta$	Effizienz der Codierung	$\eta = \frac{H(X)}{L}$
$R$	Redundanz der Codierung	$R = L - H(X)$

### 6.2 Kraft'sche Ungleichung

Gegeben ist eine Quelle mit dem Alphabet  $x_i, i = 1 \dots n$ . Jedem Symbol  $x_i$  wird eine Codelänge  $n_i$  zugewiesen. Die Kraft'sche Ungleichung besagt, dass ein eindeutig und sofort codierbarer binärer Code gefunden werden kann, wenn:

$$\sum_i 2^{-n_i} \leq 1$$

#### 6.2.1 Shannon-Fano Codierung

1. Symbole nach absteigender W'keit anordnen.
2. Mit Trennung 2 Teilmengen möglichst gleicher W'keit bilden

3. Obere Teilmenge 0, unterer Teilmenge 1 zuordnen
4. für jede Teilmenge Schritt 2 wiederholen.

### 6.3 Huffman Codierung

1. Symbole und Symbolgruppen nach absteigender W'keit anordnen.
2. Unterste zwei Symbole als Symbolgruppe zusammenfassen.
3. Weiter bei Schritt 1, bis nur noch zwei Symbolgruppen vorliegen.
4. Der Symbolgruppe mit grösserer W'keit 0, der anderen 1 zuordnen.
5. Letzte Reduktion rückgängig machen.
6. Weiter bei Schritt 4, bis für alle Einzelsymbole ein Codewort vorliegt.

## 7 Kanalcodierung

Durch das Beifügen von geeigneter Redundanz wird die Fehlererkennung und Fehlerkorrektur ermöglicht.  $C_s$  [b / Symbol]: Kanalkapazität  $H(X)$ : Entropie des DMS.

**Theorem:** Falls  $H(X) < C_s$  kann mit geeigneter Kanalcodierung die Fehlerrate der Übertragung beliebig klein gemacht werden. Falls  $H(X) > C_s$  ist fehlerfreie Übertragung nicht möglich.

Das heisst, dass Bitfehler in der Übertragung zu einer Beschränkung der nutzbaren Übertragungsrate führen.

$\underline{d}, d(x)$	Datenwort	$\underline{c}, c(x)$	Codewort
$k$	Länge des Datenwortes	$n$	Länge des Codewortes
$R_c = \frac{k}{n}$	Coderate	$m$	Anzahl Symbole im Alphabet
$\underline{s}, s(x)$	Fehlersyndrom	$K = \{0, 1\}$	Zeichen im Alphabet
$\underline{c}_r, c_r(x)$	Empfangenes Codewort	$\underline{e}, e(x)$	Error-pattern der Länge $n$

### 7.1 Blockcodes

Der Eingangsdatenstrom wird in Blöcke unterteilt, welcher separat codiert wird.

Ein **Galois Körper** ist ein algebraischer Körper mit endlich vielen Elementen. Wir beschränken uns auf den binären Fall:  $M = 0, 1$ . Die Operation  $\oplus$  (logisches XOR) und  $\odot$  (logisches AND)

$$\underline{a} = (a_1, a_2, \dots, a_n) \quad \text{und} \quad \underline{b} = (b_1, b_2, \dots, b_n) \quad \text{aus dem Code } C$$

$$\underline{c} = \underline{a} \oplus \underline{b} = (a_1 \oplus b_1, a_2 \oplus b_2, \dots, a_n \oplus b_n)$$

## 7.2 Linearer Code

Ein Code  $C$  ist genau dann linear, wenn für alle  $\underline{a}$  und  $\underline{b}$  auch  $\underline{c} = \underline{a} \oplus \underline{b}$  zu  $C$  gehört.

$w(\underline{c})$  Hamming-Gewicht: anzahl Einer des Codewortes

$d(\underline{a}, \underline{b})$  Hamming-Distanz : Anzahl unterschiedliche Stellen von  $\underline{a}$  und  $\underline{b}$

$d_{min}$  Minimale Hamming-Distanz aller möglichen Codewort-paare

$$w(\underline{c}) = d(\underline{c}, \underline{0}) \quad d(\underline{a}, \underline{b}) = w(\underline{a} \oplus \underline{b})$$

$$d_{min} = \min[d(\underline{a}, \underline{b})] \stackrel{\text{linear}}{=} \min[w(\underline{a} \oplus \underline{b})] = \min[w(\underline{c})]$$

Anhand dieser minimalen Hammingdistanz  $d_{min}$  lässt sich die Anzahl der korrigierbaren und detektierbaren Fehler berechnen:

$$t_d \quad \text{Detektierbare Fehler} \quad t_d = d_{min} - 1$$

$$t_c \quad \text{Korrigierbare Fehler} \quad t_c = \frac{1}{2} \cdot (d_{min} - 1)$$

Bei **Systematischen Blockcodes** kommen alle Datenbits unmodifiziert im Codewort vor. Falls diese Bits an einer definierten Stelle auftreten, handelt es sich um ein **geordneter systematischer Code**.

### 7.2.1 Generatormatrix $G$

$I_k$  ist die Einheitsmatrix und  $P^T$  die transponierte Paritätsmatrix.

$$\underline{c} = \underline{d} \odot G = \underline{d} \odot \begin{bmatrix} I_K & P^T \end{bmatrix}$$

$$\underline{c} = \begin{bmatrix} d_1 & d_2 & \dots & d_k \end{bmatrix} \odot \begin{bmatrix} 1 & 0 & \dots & 0 & p_{11} & p_{21} & \dots & p_{m1} \\ 0 & 1 & \dots & 0 & p_{12} & p_{22} & \dots & p_{m2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & p_{1k} & p_{2k} & \dots & p_{mk} \end{bmatrix}$$

### 7.2.2 Prätitätsprüfmatrix $H$

Mit dieser Matrix können Übertragungsfehler erkannt werden.  $O$  ist die  $[k \times m]$  Nullmatrix,  $\underline{0}$  ist der  $[1 \times m]$  Nullvektor

$$H = \begin{bmatrix} P & I_m \end{bmatrix} \quad H^T = \begin{bmatrix} P^T \\ I_m \end{bmatrix}$$

$$G \odot H^T = O \quad \underline{c} \odot H^T = \underline{d} \odot G \odot H^T = \underline{0}$$

Wenn:  $\underline{c} \odot H^T = 0 \rightarrow$  keine Fehler bei der Übertragung

Die minimale Hamming-Distanz  $d_{min}$  von  $C$  entspricht somit der minimalen Anzahl Zeilen von  $H^T$ , welche linear kombiniert den Nullvektor  $\underline{0}$  ergeben.  $\underline{c}_r$  ist das empfangene Codewort, welches maximal  $t$  Fehler haben kann, um das Codewort korrigieren zu können.

$$\underline{c}_r = \underline{c} \oplus \underline{e}$$

$$\underline{s} = \underline{c}_r \odot H^T = (\underline{c} \oplus \underline{e}) \odot H^T = \underline{c} \odot H^T \oplus \underline{e} \odot H^T = \underline{e} \odot H^T$$

Bei Einzelfehler entspricht das Fehlersyndrom  $\underline{s}$  genau einer Zeile von  $H^T$ . Wenn alle Zeilen von  $H^T$  unterschiedlich sind, kann aus  $\underline{s}$  das Fehlerbit  $e_i$  eindeutig bestimmt werden. So kann das empfangene Codewort  $\underline{c}_r$  korrigiert werden.

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

Gilt das Gleichheitszeichen, handelt es sich um einen so genannten perfekten Code. Ein perfekter Code, der nur Einzelfehler korrigieren kann, nennt man Hamming-Code.

## 7.3 Zyklische Lineare Codes

Jede Zyklische Verschiebung eines Codewortes  $\underline{c}$  zu einem neuen gültigen Codewort von  $C$  führt. Um hohe Coderate zu erzielen, sollte eine möglichst hohe Coderate  $R_c = \frac{k}{n}$  erreicht werden. Ein Codewort  $\underline{c}$  kann als Polynom  $c(x)$  geschrieben werden:

$$\underline{c} = (c_0, c_1, c_2, \dots, c_{n-1}) \quad c(x) = c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1}$$

Es werden folgende Operationen definiert:

$$\text{mod } 2(x^k + x^k) = x^k \oplus x^k = 0 \quad \text{mod } 2(x^k - x^k) = x^k \ominus x^k = 0$$

$$\text{mod } 2(0 + x^k) = 0 \oplus x^k = x^k \quad \text{mod } 2(0 - x^k) = 0 - x^k = x^k$$

Beispiele:  $\underline{a} = (11000) \quad a(x) = 1 + x + x^2$   
 $\underline{b} = (10110) \quad b(x) = 1 + x^2 + x^3$

$$\underline{a} \odot \underline{b} = a(x) \cdot b(x) = 1 + x + 2x^2 + 2x^3 + 2x^4 + x^5 = 1 + x + x^5 \Rightarrow (11001)$$

Im Folgenden wird eine wichtige Operation beschrieben. Für das Polynom  $q(x)$  interessiert man sich meist nicht. Normalerweise wird nach dem Rest  $r(x)$  gesucht.  $r(x)$  und  $q(x)$ . Die Operation  $\odot$  ist eine Polynomdivision.

$$f(x) = q(x) \cdot h(x) + r(x) \quad f(x) \odot h(x) \Rightarrow q(x), r(x)$$

$$\text{Notation:} \quad r(x) = f(x) \text{ mod } h(x)$$

Wenn ein Codewort  $c$  um  $i$  Stellen zyklisch verschoben wird:

$$\underline{c}^{(i)} = (c_{n-i}, c_{n-(i-1)}, \dots, c_{n-1}, c_0, c_1, \dots, c_{n-(i+1)})$$

$$c^{(i)}(x) = c_{n-i} + c_{n-(i-1)}x + \dots + c_{n-1}x^{i-1} + c_0x^i + c_1x^{i+1} + \dots + c_{n-(i+1)}x^{n-1}$$

$$c^{(i)}(x) = x^i c(x) \text{ mod } (1 + x^n)$$

### 7.3.1 Fundamentales Theorem für zyklische Codes

Gegeben sei das Generatorpolynom  $g(x)$  mit der Ordnung  $(n - k)$ . Jeder  $(n, k)$  zyklische Code  $C$  kann mit Hilfe eines solchen Polynoms  $g(x)$  gebildet werden:

$$\text{Bedingungen:} \quad g_{n-k} = g_0 = 1 \quad (x^n + 1) = q(x) \odot g(x) \quad (\text{ohne Rest})$$

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

### 7.3.2 Fehlersyndrom

Im empfangenen Codewort  $c_r(x)$  muss der Fehler  $e(x)$  gefunden werden. Das Fehlersyndrom  $s(x)$  ist ein Polynom des Grads  $n - k$ .

$$c_r(x) = c(x) \oplus e(x)$$

$$s(x) = r(x) \text{ mod } g(x)$$

$$s(x) = e(x) \text{ mod } g(x)$$

### 7.3.3 Generatormatrix

$$G = \begin{pmatrix} g(x) \\ x \cdot g(x) \\ x^2 \cdot g(x) \\ \vdots \\ x^{k-1} \cdot g(x) \end{pmatrix}$$

### 7.3.4 Hardware-Realisierung

$$\text{Generatorpolynom} \quad g(x) = g_0 + g_1x + g_2x^2 + \dots + g_{n-k}x^{n-k}$$

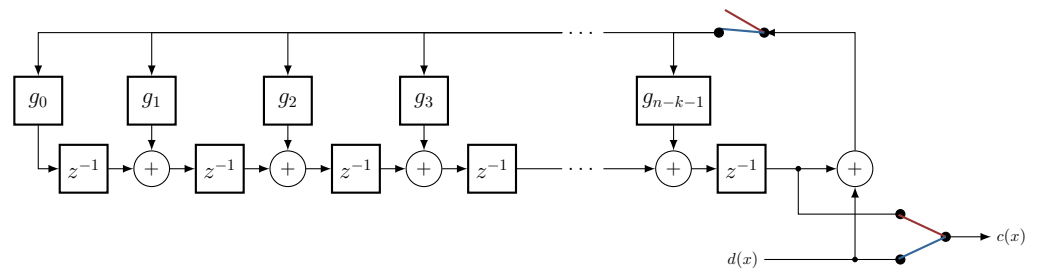
$$\text{Datenwort} \quad d(x) = d_0 + d_1x + d_2x^2 + \dots + d_{k-1}x^{k-1}$$

$$\text{Parity Bits} \quad p(x) = p_0 + p_1x + p_2x^2 + \dots + p_{n-k-1}x^{n-k-1}$$

$$\text{Codewort} \quad c(x) = p_0 + \dots + p_{n-k-1}x^{n-k-1} + d_0x^{n-k} + \dots + d_{k-1}x^{n-1}$$

$$c(x) = q(x) \cdot g(x) = p(x) + x^{n-k} \cdot d(x)$$

$$x^{n-k} \cdot d(x) = q(x) \cdot g(x) + p(x)$$



- **Phase 1:** Ausgabe von  $d(x)$ . ( $k$  Zyklen)
- **Phase 2:** Ausgabe von  $p(x) = \text{Rest}$ . ( $n - k$  Zyklen)