

# 1 Einführung

## 1.1 Struktur von Kommunikationsnetzen

- Teilnehmernetz
- Zugangnetz (access network): wireless, wireline
- Weitverkehrsnetze

## 1.2 Codierungsarten

<b>Quellcodierung</b> redundanzbehalteter Code wird optimiert
<b>Kanalcodierung</b> hinzufügen nützlicher Redundanz: Prüfbits
<b>Leitungscodierung</b> geeignete Signaldarstellung $\Rightarrow$ Maximierung der Ü-Geschwindigkeit

# 2 Grundzüge der Wahrscheinlichkeitsrechnung

## 2.1 Zufallsereignis und Wahrscheinlichkeit

$\Omega$ : Ergebnisraum $\omega_j$ : Versuchsergebnis Wahrscheinlichkeit als Grenzwert der relativen Häufigkeit: $h(A_i) = \frac{n_i}{n} \Rightarrow P(A_i) = \lim_{n \rightarrow \infty} \frac{n_i}{n}$
<b>Eigenschaften</b> - $0 \leq P(A_i) \leq 1$ - $A_i \cap A_j = \emptyset \Rightarrow P(A_i \cup A_j) = P(A_i) + P(A_j)$ - $\sum P(A_i) = 1$
<b>Vollständiges Ereignissystem</b> : disjunkte Ereignisse die $\Omega$ ergeben <b>Verbundereignis</b> : $(A \cap B) = (A, B)$ <b>Bedingte Wahrscheinlichkeit</b> : $(A   B)$ : Eintritt von A unter Bedingung B $P(A   B) = \frac{P(A, B)}{P(B)}$ <b>Statistische Unabhängigkeit</b> : $P(A, B) = P(A) \cdot P(B)$ (z.B. bei Bitfolgen)

## 2.2 Zufallsvariable, Verteilung und Verteilungsfunktion

<b>Zufallsvariable</b> - diskret: meist nur ganzzahlige Werte - kontinuierlich: reellwertig
<b>Verteilung</b> X: diskrete ZV, $x(i) = P(X = i)$ $\sum x(i) = 1$ Verteilungsfunktion: treppenförmig
<b>Bernoulli-Versuch &amp; -Verteilung</b> Experiment mit zwei möglichen Ergebnissen $y(i) = P(Y = i) = \begin{cases} q & i = 0 \text{ Mißerfolg} \\ 1-q & i = 1 \text{ Erfolg} \end{cases}$
<b>Binomial-Verteilung</b> Anzahl N von Bernoulli-Versuchen: $x(i) = P(X = i) = \binom{N}{i} (1-q)^i q^{N-i}, i = 0, 1, \dots, N$  Bsp: Wahrscheinlichkeit für i Bitfehler im Paket $x(i) = \binom{n}{i} p_b^i (1-p_b)^{n-i}$ Paketfehlerwahrscheinlichkeit $p_p = \sum x(i) = 1 - (1-p_b)^n \approx 1 - (1-n \cdot p_b) = n \cdot p_b$ (für $p_b \gg 1$ )
<b>Geometrische Verteilung</b> Wiederholung von Bernoulli-Versuchen bis zum ersten Erfolg (Wk 1-q) $x(i) = P(X = i) = q^i (1-q), i = 0, 1, \dots$ Bsp: Übertragungsstrecke mit Paketfehlerwahrscheinlichkeit $p_p$ $x(i) = p_p^i (1-p_p)$
<b>Verteilungsfunktion</b> A: beliebige ZV: $A(t) = P(A \leq t)$ - $t_1 < t_2 \Rightarrow A(t_1) \leq A(t_2)$ - $t_1 < t_2 \Rightarrow P(t_1 < A \leq t_2) = A(t_2) - A(t_1)$ - $A(-\infty) = 0, A(\infty) = 1$ Verteilungsdichtefunktion: $a(t) = \frac{d}{dt} A(t)$ Vollständigkeitsrelation: $\int_{-\infty}^{\infty} a(t) dt = 1$

## 2.3 Erwartungswert und Momente

### Erwartungswert

$$E[g(A)] = \int_{-\infty}^{\infty} g(t) \cdot a(t) dt$$

### Mittelwert

$$g(A) = A \Rightarrow m_1 = E[A] = \int t \cdot a(t) dt$$

### Gewöhnliche Momente

$$g(A) = A^k \Rightarrow m_k = E[A^k] = \int t^k \cdot a(t) dt$$

### Zentrale Momente

$$g(A) = (A - m_1)^k \Rightarrow \mu_k = E[(A - m_1)^k] = \int (t - m_1)^k \cdot a(t) dt$$

$$\text{Varianz: } \text{VAR}[A] = \mu_2 = m_2 - m_1^2 \text{ (sec}^2\text{)}$$

$$\text{Standardabweichung: } \sigma_A = \sqrt{\text{VAR}[A]} \text{ (sec)}$$

$$\text{Variationskoeffizient: } c_A = \frac{\sigma_A}{m_1} = \frac{\sqrt{\text{VAR}[A]}}{E[A]}$$

### 3 Fehlererkennung und Fehlerkorrektur

#### 3.2 Grundprinzip der Kanalcodierung

X: Quellcodewort (Nutzbits)  
 $\Gamma$  Vorschrift zur Berechnung der nützlichen Redundanz  
Y: nützliche Redundanz (Prüfbits)  
(X,Y): gesendetes Codewort  
  
( $X^*, Y^*$ ): empfangenes Codewort, evtl. störungsbehaftet  
Y: vom Empfänger neu berechnete nützliche Redundanz

- Automatische Fehlerkorrektur (größere Restwahrscheinlichkeit Fehlerkorrektur und -erkennung beim Empfänger)
- Wiederholungsaufforderung (NAK und ACK)  
Rückkanal erforderlich

#### 3.3 Coderaum

**Parity Check**  
Coderaum: alle möglichen Codewörter:  $2^{m+1}$  CW benutzte Codewörter:  $2^m$

- sichere Erkennung ungerader Fehlerzahl
- keine Erkennung gerader Fehlerzahl
- keine automatische Korrektur möglich

Ziel: benutzte CW so weit wie möglich auseinander platzieren

**Hamming-Distanz**  
Code mit  $n = m + k$  Stellen  
Distanz von  $x_i, x_j$  benutzte CW:  $d(x_i, x_j)$  (Anzahl unterschiedlicher Binärstellen)  
Hamming-Distanz  $h = \min\{d(x_i, x_j)\} \forall i, j$   
Anzahl sicher erkennbarer Fehler:  $\eta = h - 1$   
Anzahl sicher korrigierbarer Fehler:  $\eta = \frac{h-2}{2}$  (h gerade),  $\eta = \frac{h-1}{2}$  (h ungerade)

### Dichtgepackter Code

Anzahl der CW pro Korrigierbereich:  $\sum_{i=0}^{\eta} \binom{n}{i}$

Anzahl aller CW  $2^m \sum_{i=0}^{\eta} \binom{n}{i}$

Code dichtgepackt: Anzahl =  $2^n$  (keine CW außerhalb der Korrigierbeiche)

### Hamming-Grenze:

allg:  $2^m \sum_{i=0}^{\eta} \binom{n}{i} \leq 2^n$

$k \geq \log_2 \left( \sum_{i=0}^{\eta} \binom{n}{i} \right) = \text{ld} \left( \sum_{i=0}^n \binom{m+n}{i} \right)$

Code-Effizienz:  $\frac{m}{n}$

### 3.4 Restfehlerwahrscheinlichkeit

- Restfehler bei automatischer Korrektur

Restfehler: Verfälschung von  $x_i$  in ein CW außerhalb des Korrigierbeichs von  $x_i$

$$P_{RK} = P(> \eta \text{ Fehler}) = 1 - \sum_{i=0}^{\eta} \binom{n}{i} p_b^i (1 - p_b)^{n-i}$$

Für  $p_b \ll 1, \eta \ll n \Rightarrow P_{RK} \approx 1 - e^{-np_b}$

- Restfehler bei Wiederholungsaufforderung

Restfehler: Verfälschung von  $x_i$  in ein anderes benutztes CW  $x_j$

$$\text{Näherung } P_{RN} = \frac{\text{Anzahl anderer benutzter CW}}{\text{Anzahl aller anderer CW}} = \frac{2^m - 1}{2^n - 1} \approx 2^{-k}$$

$\Rightarrow P_{RK} > P_{RN}$

## 4 Algebra der Restklassen

### 4.1 Modulo-Rechnung und Restklassen

#### Rechnung Modulo-M

$a \pmod{M}$ : Rest nach ganzzahliger Division durch M

Die Restklassen sind vollständig durch den jeweiligen Rest gekennzeichnet:  
 $0, 1, \dots, M - 1$

**Gruppe:** Axiome 1-4

**Ring:** Axiome 1-8

**Körper:** Axiome 1-11

Axiom 1: Summe  $a+b$  definiert und wieder in Menge

Axiom 2: Assoziativgesetz:  $(a + b) + c = a + (b + c)$

Axiom 3: Nullelement 0:  $a + 0 = a$

Axiom 4: Jedes Element besitzt additiv inverses  $a_{-1}$  mit  $a + a_{-1} = 0$

Axiom 5: Summe kommutativ  $a + b = b + a$

Axiom 6: Produkt  $a \cdot b$  definiert und wieder in Menge

Axiom 7: Assoziativgesetz:  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

Axiom 8: Distributivgesetz:  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Axiom 9: Produkt kommutativ  $a \cdot b = b \cdot a$

Axiom 10: Einselement 1:  $a \cdot 1 = a$

Axiom 11: Jedes  $a \neq 0$  hat multiplikativ inverses  $a^{-1}$  mit  $a \cdot a^{-1} = 1$

- Die Rechnung  $(\text{mod } M)$  bildet einen Körper, falls M eine Primzahl ist
- M keine Primzahl: Rechnung  $(\text{mod } M)$  bildet Ring
- Es entstehen Zyklen (auch Teilzyklen)

### 4.2 Lineare Gleichungen in der mod-M-Rechnung

- Die Vektoren  $X_1, X_2, \dots, X_n$  sind linear unabhängig, falls die Ungleichung  $c_1 X_1 + c_2 X_2 + \dots + c_n X_n \neq 0$  ( $c_i = 0, 1$ ) für jeden Wahl der  $c_i$  erfüllt ist (außer für alle  $c_i = 0$ )

### 4.3 Modulo-Rechnung für Polynome

#### Polynome

$$P(u) = c_r u^r + c_{r-1} u^{r-1} + \dots + c_1 u^1 + c_0 u^0 \quad (c_i \in \{0, 1\})$$

- Es existieren  $2^{r+1}$  Polynome vom Grad  $r$
- $P(u)$  reduzibel, falls aufspaltbar:  $P(u) = P_1(u) \cdot P_2(u)$
- $P(u)$  irreduzibel, falls nicht weiter zerlegbar
- Polynomdivision mittels 1 und 0
- Die Restpolynome bei der Rechnung (mod  $M(u)$ ): Modularpolynome, Grad  $r$  bilden einen endlichen Körper aus  $2^r$  Elemente genau dann wenn  $M(u)$  ein irreduzibles Polynome vom Grad  $r$  ist

### 4.4 Zyklische Eigenschaft der Potenzrestklassen

- **Periode eines Polynoms**

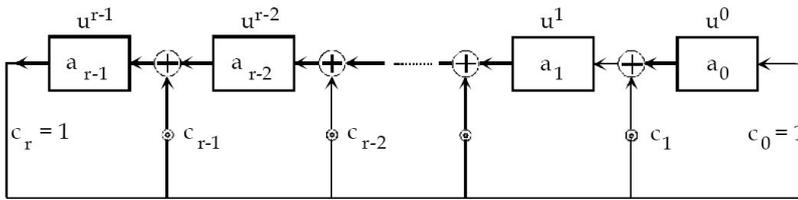
$M(u)$  vom Grad  $r$  hat  $2^r$  Restklassen, betrachtet wird  $[u^i](\text{mod } M(u))$

**Periode** ist kleinste positive Zahl für die  $u^p = u^0(\text{mod } M(u)) = 1$

Periode ist somit auch die kleinste positive Zahl, für die das Polynom  $(u^p + 1)$  das Polynom  $M(u)$  als Faktor enthält

- $p_{max} = 2^r - 1$
- Ein Polynom vom Grad  $r$ , dass Periode  $p_{max}$  erreicht heißt **primitiv**

Ein primitives Polynom ist immer irreduzibel



**Polynombeschreibung für rückgekoppelte Schieberegister**

r FlipFlops (Speicherung von 0 oder 1)

Rückkopplungsmuster  $M(u) = \sum_{i=0}^r c_i u^i = 1 \cdot u^r + c_{r-1} u^{r-1} + \dots + c_1 u^1 + 1 \cdot u^0$

**Übergangsverhalten des Schieberegisters:  $SR(n) \Rightarrow SR(n+1)$**

$a_i(n+1) = a_{r-1}(n) \cdot c_i + a_{i-1}(n)$

$a_0(n+1) = a_{r-1}(n)$

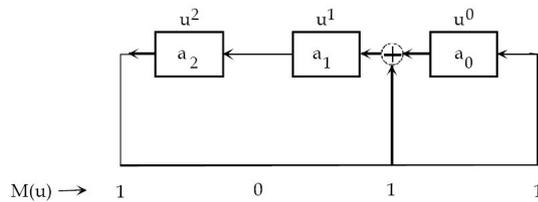
Genauer:  $SR(n+1) = SR(n) \cdot u \pmod{M(u)}$

**Realisierung der Zyklen**

Operation des SR entspricht Polynommultiplikation mit  $u \pmod{M(u)}$ , wobei  $M(u)$  das Polynom des Rückkopplungsmusters ist

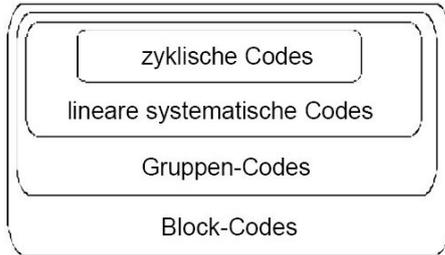
- falls  $SR(n) = 0 \Rightarrow SR(n+1) = 0 \cdot u = 0$  (Nullzyklus)
- falls  $SR(n) = u^i \Rightarrow SR(n+1) = u^{i+1}$  (Zyklus der Potenz Restklassen)
- $M(u)$  primitiv  $\Rightarrow$  maximale Periode wird erreicht
- $M(u)$  nicht-primitiv  $\Rightarrow$  Unterzyklen werden durchlaufen, je nach  $SR(n)$

Beispiel Rückkopplungspolynom  $M(u) = u^3 + u + 1 \equiv 1\ 0\ 1\ 1 \quad (r=3)$



## 5 Blockcodes und Gruppencodes

### 5.1 Einteilung



### 5.2 Blockcodes

- binäre CW mit konstanter Codewortlänge
- Summe zweier CW: Vektoraddition (mod 2)
- **Gewicht**  $w(CW_i)$ : Anzahl der Einsen
- **Gewichtverteilung**  $A(w)$  Anzahl der CW mit Gewicht  $w = 0, 1, \dots, n$
- **Distanz**  $d(CW_i, CW_j) = w(CW_i + CW_j)$
- **Hamming Distanz**:  $h = \min_{i \neq j} (d(CW_i, CW_j))$
- **Distanzverteilung**  $B(d, CW_i)$   
Anzahl der CW, die von Ausgangswort Distanz d aufweisen

### 5.3 Binäre Gruppencodes

binärer Gruppencode entsteht durch Linearkombination aus den m Nutzbits des Codewortzeichens und den m Generatorworten

- m linear unabhängige Generatorwort  $G_1, G_2, \dots, G_m$  mit  $G_i = \{g_{i1}, g_{i2}, \dots, g_{in}\}$

- $CW_i = \xi_{i1}G_1 + \xi_{i2}G_2 + \dots + \xi_{im}G_m$

Beispiel	$\odot$	0	1	0	1	1	$G_1$	mit Generatormatrix	
	$\odot$	1	0	1	1	0	$G_2$		
i	$\xi_{i1}$	$\xi_{i2}$							$G = \begin{pmatrix} G_1 \\ G_2 \\ \vdots \\ G_m \end{pmatrix}$ und $CW_i = (\xi_{i1}\xi_{i2} \dots \xi_{im}) \cdot G$
0	0	0	0	0	0	0	$CW_0$		
1	0	1	0	1	1	0	$CW_1$		
2	1	0	1	0	1	1	$CW_2$		
3	1	1	1	1	0	1	$CW_3$		

- CW des binären Gruppencodes bilden Gruppen
- $b(d, CW_A) = A(w) \Rightarrow$  Distanzverteilung gleich für alle CW

## 5.4 Lineare systematische Binärcodes

<p>Trennung von <math>m</math> Nutzbits und <math>k</math> Kontrollbits          Berechnung der Nutzbits mittels linearer Gleichungen (mod 2) gemäß eines Prüfschemas          Prüfmatrix <math>P</math></p> $\left( \begin{array}{cccc ccc} x_1 & x_2 & x_3 & x_4 & y_5 & y_6 & y_7 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{array} \right)$ <p><math>P \cdot (XY)^T = 0^T</math>  <math>W(F) = 1 \Rightarrow</math> Fehler erkennbar und korrigierbar  <math>W(F) = 2 \Rightarrow</math> Fehler erkennbar <math>\Rightarrow \eta = 1</math></p>
--

- Wichtig: Element aus Prüfspalte muss kein Codewort sein
- Ermittlung des Fehlersyndroms:  $Y^{*T} + Y'^T$  ergibt gefälschte Stelle
- Fehlermuster  $(XY) + (F) = (X^*Y^*)$   
 Fehlersyndrom  $Z = P \cdot F^T$

<p>Hamming-Distanz <math>h \Rightarrow \bar{\eta} = h - 1</math> Fehler erkennbar          Bei einem linearen systematischen Code mit Hamming-Distanz <math>h</math> sind <math>h-1</math> beliebig herausgewählte Prüfspalten linear unabhängig</p>
--

<p><b>Spezialfall <math>h = 3</math></b></p> <ul style="list-style-type: none"> <li>• alle Prüfspalte <math>\neq 0</math></li> <li>• alle Paar von Prüfspalten linear unabhängig</li> </ul> <p>Aufstellung für <math>h &gt; 3</math> problematisch (wg. Bed.: <math>h-1</math> bel. Prüfspalten l.u.)</p>
---

<p><b>Korrigierbarkeit von Fehlern</b>          Fehler korrigierbar, falls paarweise Zuordnung <math>F_i \leftrightarrow Z_i</math> möglich und eindeutig ist</p> <p>notwendige Bedingung für Korrigierbarkeit von <math>\eta</math> Fehlern</p> $2^k - 1 \geq \sum_{i=1}^{\eta} \binom{n}{i}$
--

<p><b>Erkennbarkeit von Fehlern</b>          Für <math>\eta = 2</math> müsste für Fehlersyndrome <math>W(F) = 1, \binom{n}{1}</math> und <math>W(F) = 2, \binom{n}{2}</math> gelten          Anzahl erzeugbarer Prüfspalten <math>2^k - 1 \geq \binom{n}{1} + \binom{n}{2}</math></p>
---

## 6 Zyklische Codes und Anwendung

### 6.1 Codierungsvorschrift

die **Generatorworte** entstehen aus einem Generatormuster gemäß eines Generatorpolynoms durch  $m-1$  Verschiebungen des Generatormusters

$$CW_I = \xi_{i1}G_1 + \xi_{i2}G_2 + \dots + \xi_{im}G_m$$

mit  $\xi_{ii}$  Nutzbits und  $G_i$  Generatorworte aus je  $n$  Stellen

Generatorworte sind linear unabhängig voneinander

#### Polynomdarstellung für Codeworte

$$CW_i(u) = G(u)[\xi_{i1} \cdot u^0 + \xi_{i2} \cdot u^1 + \dots + \xi_{im} \cdot u^{m-1}] = G(u) \cdot Q_i(u)$$

$$\text{allgemein } \boxed{CW(u) = G(u) \cdot Q(u)}$$

#### Erzeugung der Prüfstellen

Trennung von Nutzbits und Prüfbits

Nutzbits  $X(u)$  und  $k$  Prüfbits

$$\text{Codewort } \boxed{CW(u) = X(u) \cdot u^k + R(u) = G(u) \cdot Q(u)}$$

$R(u)$  ist Rest der Division  $\frac{X(u) \cdot u^k}{G(u)}$

### 6.2 Äquivalenz von Prüfschema und zyklischen Codes

$$\boxed{CW(u) = 0 \pmod{G(u)}}$$

$$x_1u^{n-1} + x_2u^{n-2} + \dots + x_mu^k + y_{m+1}u^{k-1} + \dots + y_nu^0 = 0 \pmod{G(u)}$$

$$\text{Für die Prüfspalten } u^{n-i} \pmod{G(u)} = P_i = \begin{pmatrix} A_{i,k-1} \\ \vdots \\ a_{i,1} \\ a_{i,0} \end{pmatrix} \leftarrow \begin{matrix} \text{Wertigkeit} \\ u^{k-1} \\ \vdots \\ u^1 \\ u^0 \end{matrix}$$

Schließlich erhält man ein Prüfschema:

$$x_1P_1 + x_2P_2 + \dots + x_mP_m + y_{m+1}P_{m+1} + \dots + y_nP_n = 0^T$$

$\Rightarrow$  Äquivalenz Prüfschema und zyklischer Code

#### $G(u)$ primitiv

$u^i \pmod{G(u)}$  ist zyklisch mit  $n = p_{\max} = 2^k - 1$

#### Satz

Die durch zyklische Verschiebung aus einem CW erzeugten Worte sind ebenfalls CW

Beweis: Verschiebung  $u \cdot CW(u)$  liefert gültiges CW

**Fehlererkennung**Fehlervektor  $F = (f_1 \dots f_n)$ Fehlersyndrom  $Z = f_1 P_1 + \dots + f_n P_n$  $CW(u) = 0 \pmod{G(u)} \Rightarrow Z(u) = F(u) \pmod{G(u)}$ 

Fehlersyndrom ist nur vom Fehlermuster abhängig nicht vom CW selber

Fehler *erkennbar*, falls  $F(u) \neq 0 \rightarrow Z(u) \neq 0$ Fehler nicht erkennbar, falls  $F(u)$  ein CW darstellt**6.3 Zyklische Hamming-Codes**

- zyklischer Code mit Generatorpolynom  $G(u)$  (primitiv, Grad  $k$ )
- Codewortlänge  $n = 2^k - 1$
- Hamming-Distanz  $h=3$
- Prüfschema durch Polynomdivision

**6.4 Weitere zyklische Codes****Zyklische Abramson-Codes**zyklischer Code mit  $G(u) = G_1(u)(u + 1)$ ,  $G_1(u)$  primitiv, Grad  $k_1$  $h = 4, \eta = 1, \bar{\eta} = 3$ Prüfschema: Prüfspalte  $P_i$  ist äquivalent zur  $u^{n-i} \pmod{G(u)}$ **Fire-Code (Büschelfehler erkennen)** $G(u) = G_1(u) \cdot (u^{k_2} + 1)$ ,  $G_1(u)$  primitiv, Grad  $k_1$ , Periode  $p_1$  $n = kgV(p_1, K_2)$ Fehlererkennung von Büschelfehler der Länge  $b < \frac{k_2}{2} + 1$  und  $b \leq k_1$ **BCH-Code**Codes mit vorgegebbarer Hamming-Distanz ( $\eta$  Fehler sicher korrigierbar) $G(u) = G_1(u) \cdot G_2 \dots G_\eta(u)$  $G_1$  primitiv,  $G_2(u), \dots, G_\eta(u)$  aus  $G_1(u)$  abgeleitet $n = 2^{k_1} - 1$

## 6.5 Schaltungsrealisierungen

<b>Codierschaltung nach Prüfmatrix mittels XOR</b>
<b>Codierschaltung mit rückgekoppeltem Schieberegister</b> $SR(i+1) = SR(i) \cdot u \pmod{G(u)}$ Erweiterung: zum Takt $i$ steht das Nutzbit $x_{i+1}$ am Eingang an $\Rightarrow SR(i+1) = u \cdot SR(i) + x_{i+1}u^k \pmod{G(u)}$  $SR(0) = 0$ $SR(1) = SR(0) \cdot u + x_1u^k$ $SR(2) = SR(1) \cdot u + x_2u^k = x_1u^{k+1} + x_2u^k$ $SR(3) = x_1u^{k+1} + x_2u^{k+1} + x_3u^k$ $\vdots$ $SR(m) = x_1u^{k+m-1} + x_2u^{k+m-2} + \dots + x_mu^k \pmod{G(u)}$ $= y_{m+1}u^{k+1} + \dots + y_nu^0$  $\Rightarrow$ Nach $m$ Takten stehen die Prüfbits im SR
<b>Decodierschaltungen</b> $CW^*(u) = CW(u) + F(u)$ (Fehler) $SR(i+1) = u \cdot SR(i) + (x_{i+1} + f_{i+1})u^k \pmod{G(u)}$  $SR(0) = 0$ $SR(1) = (x_1 + f_1)u^k$ $\vdots$ $SR(n) = (x_1 + f_1)u^{n+k-1} + (x_2 + f_2)u^{n+k-2} + \dots + (x_n + f_n)u^k$ $= u^k(CW(u) + F(u)) \pmod{G(u)}$ $= u^kF(u) \pmod{G(u)}$ $= u^kZ(u) \pmod{G(u)}$  $\Rightarrow$ nach $n$ Takten steht das Fehlersyndrom (um $k$ Stellen verschoben im SR)

## 7 Nachrichtenquelle und Informationsgehalt

### 7.1 Codebaum und Entscheidungsaufwand

Quelle	→	Ü-Kanal	→	Senke		
		Störung				
Codewort		$a_{n-1}$	$a_{n-2}$	$\dots$	$a_1$	$a_0$
Basen		$z_{n-1}$	$z_{n-2}$	$\dots$	$z_1$	$z_0$
Codebaum (Reihenfolge der Entscheidungen) liefert Wertebereich(Codeumfang)						
Wertebereich		$N = \prod_{i=0}^{n-1} z_i$		Problem: Wie sind $z_i$ zu wählen, so dass H bei		
Entscheidungsaufwand		$H = \sum_{i=0}^{n-1} z_i$		konstantem N minimal wird?		
mit einheitlicher Basis für alle CW-Stellen						
⇒ Entscheidungsaufwand minimal, wenn Einheitsbasis $z = z_i = e$						

### 7.2 Entscheidungsgehalt und Informationsgehalt

<b>Entscheidungsgehalt</b> In Digitaltechnik zweiwertige Logik Zeichenvorrat: ⇒ $N = 2^n$ Entscheidungsgehalt: Anzahl der Entscheidungen $n = \text{ld } N$ [bit]
Auftrittswk. für $x_i : p(x_i)$ mit $\sum p(x_i) = 1$ <b>Informationsgehalt</b> $I_i = C \text{ld}(p(x_i))$ mit C Normierungskonstante binäre Quelle mit 2 Zeichen soll einem Informationsgehalt von 1 bit entsprechen, deshalb $1 = C \text{ld}0,5 \Rightarrow C = -1$ $I_i = -\text{ld}(p(x_i)) = \text{ld} \frac{1}{p(x_i)}$ Erwartungswert von I: $H^* = E[I] = \sum_{i=1}^n p(x_i) \text{ld} \frac{1}{p(x_i)}$ ⇒ Additivität $I_{i,j} = I_i + I_j$ gewährleistet
<b>Maximaler Informationsgehalt der Quelle</b> $H_{max}^* = \sum_{i=1}^N p(x_i) \text{ld} \frac{1}{p(x_i)} = \sum_{i=1}^N \frac{1}{N} \text{ld} \frac{1}{1/N} = \text{ld} N = H_0$

### 7.3 Redundanzreduzierende Codierung

$S_i$ Binäre Stellenzahl für $x_i$ mittlere Codewortlänge: $S_m = \sum p(x_i)S_i$
<b>Satz von Shannon</b> Code existiert mit $ld \frac{1}{p(x_i)} \leq S_i \leq ld \frac{1}{p(x_i)} + 1$
<b>Redundanz</b> $R_c = S_m - H^*$ ( $S_m$ : tatsächlicher Aufwand; $H^*$ theoretischer Minimalaufwand)
<b>Codierung nach Shannon und Fano</b>  <ol style="list-style-type: none"><li>1. <math>x_i</math> ordnen nach fallenden Auftrittswahrscheinlichkeiten</li><li>2. fortgesetzte Einteilung möglichst gleicher Wahrscheinlichkeitsanteile</li></ol>
<b>Codierung nach H</b>  <ol style="list-style-type: none"><li>1. <math>x_i</math> ordnen nach fallenden Auftrittswahrscheinlichkeiten</li><li>2. Die beiden kleinstwahrscheinlichen Zeichen x,y werden zur Unterscheidung mit 0 und 1 codiert</li><li>3. Die beiden Zeichen x und y werden zu einem neuen Zeichen xy zusammengefasst. Neues Zeichen wird die Summe der Wahrscheinlichkeiten der ursprünglichen Zeichen zugeordnet. Nur noch ein Zeichen übrig: Schritt 4, sonst Schritt 1</li><li>4. Aufstellen des Codebaums: Endknoten liefern Codierung</li></ol>

## 8 Informationstheorie in Übertragungssystemen

### 8.1 Entropie in Übertragungssystemen

#### Modell eines Ü-Kanals

$p(y_j | x_i)$  Bedingte WK, dass  $y_j$  empfangen wird, vorausgesetzt  $x_i$  wurde gesendet  
 $p(y_j, x_i)$  (Verbund-)WK, dass  $x_i$  gesendet und  $y_j$  empfangen werden

Sender 
$$p(x_i) = \sum_{j=1}^M p(x_i, y_j)$$

Empfänger 
$$p(y_i) = \sum_{i=1}^N p(x_i, y_j)$$

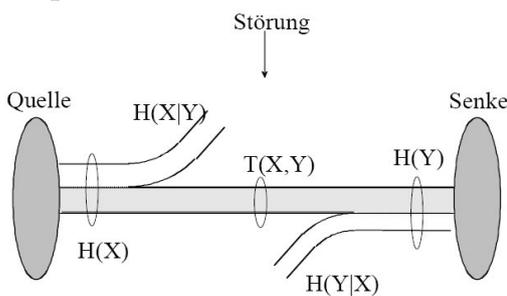
$$p(x_i, y_j) = p(x_j | x_i) \cdot p(x_i) = p(x_i | y_j) \cdot p(y_j)$$

mit  $p(x_i | y_j)$  Rückschluss-Wahrscheinlichkeit  
 und  $p(y_j | x_i)$  Vorhersage-Wahrscheinlichkeit

ungestörter Ü-Kanal 
$$p(x_i | y_j) = \begin{cases} 0 & j \neq i \\ 1 & j = i \end{cases}$$

gestörter Ü-Kanal  $p(y_j | x_i) = p(y_j)$ , d.h.  $y_j$  tritt unabhängig von  $x_i$  auf

#### Entropie



Informationsgehalt der Quelle  $H(X) = H^*$

Informationsgehalt der Senke  $H(Y)$

Rückschluss-Entropie 
$$H(X | Y) = \sum_{i=1}^N \sum_{j=1}^M p(x_i, y_j) \cdot \text{ld} \frac{1}{p(x_i | y_j)}$$

Vorhersage-Entropie 
$$H(Y | X) = \sum_{i=1}^N \sum_{j=1}^M p(x_i, y_j) \cdot \text{ld} \frac{1}{p(y_j | x_i)}$$

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

ungerstörter Ü-Kanal  $H(Y | X) = 0$

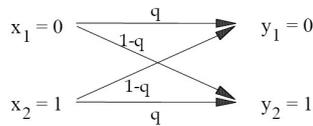
stark gestörter Ü-Kanal  $H(Y | X) = H(Y)$

**Transinformationsgehalt** (Maß für den tatsächlichen Informationsfluss)

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

## 8.2 Der symmetrische binäre Übertragungskanal

### Modell eines symmetrischen Binärkanals



**Maximaler Informationsgehalt bei**

$$p(x_1) = p(x_2) = \frac{1}{2}$$

**Verbundwahrscheinlichkeit**

$$p(x_1, y_1) = p(x_2, y_2) = \frac{q}{2}$$

$$p(x_1, y_2) = p(x_2, y_1) = \frac{1-q}{2}$$

**Auftrittswahrscheinlichkeit am Empfänger**

$$p(y_1) = p(y_2) = \frac{1}{2}$$

**bedingte Wahrscheinlichkeit am Sender**

$$p(x_1 | y_1) = q$$

$$p(x_1 | y_2) = 1 - q$$

**Kanalkapazität**

$$T(X, Y) = 1 - q \operatorname{ld} \frac{1}{q} - (1 - q) \operatorname{ld} \frac{1}{1-q}$$

Transinformationsgehalt auch 1, falls  $p_b = 1$

Transinformationsgehalt minimal bei  $p_b = \frac{1}{2}$

Bitübertragungsdauer  $t_{bit} = \frac{1}{C}$

**maximale Kanalkapazität**

$$C^* = \frac{T(X, Y)}{t_{bit}} = T(X, Y) \cdot C \text{ in } \frac{\text{bit}}{\text{Zeiteinheit}}$$

maximale Kanalkapazität des kontinuierlichen (analogen) Kanals (nach SHANNON)

$$C^* = B \operatorname{ld} \left( 1 + \frac{p_s}{p_n} \right), \text{ wobei}$$

B: Bandbreite in Hz

$\frac{p_s}{p_n}$  Verhältnis Signal-Geräusch-Leistung

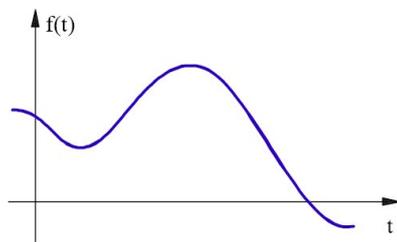
## 9 Signaldarstellung in Übertragungssystemen

### 9.1 Elemente digitaler Signalübertragung

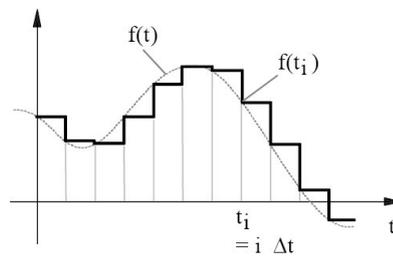
- Analoges Signal (Darstellung im Frequenzbereich, Fourier-Transformation)
- abgetastetes Signal (Nyquist-Kriterium)
- Abtastproben: Quantisierung
- digitale Darstellung der Abtastproben - Multiplexbildung
- leitungscodeiertes Signal

### 9.2 Signaldarstellung im Zeit- und Frequenzbereich

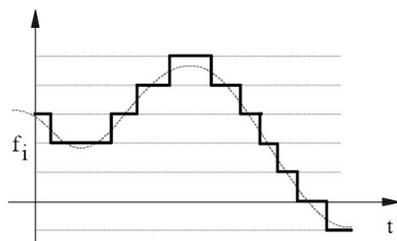
#### Basisbandsignale



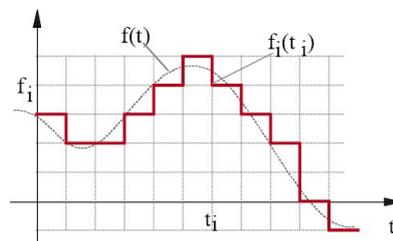
$f(t)$ : wert- und zeitkontinuierliches Signal



$f(t_i)$ : wertkontinuierliches, zeitdiskretes Signal



$f_1(t)$ : wertdiskretes, zeitkontinuierliches Signal



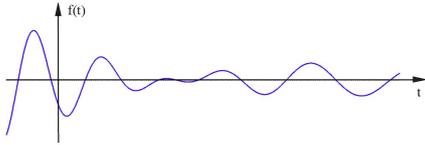
$f_1(t_i)$ : wert- und zeitdiskretes Signal

#### Modulierte Signale

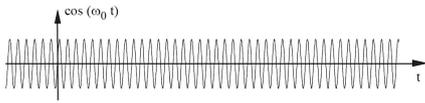
Modulation: Anpassung der Signalform an die Eigenschaften des Übertragungskanal

## Amplitudenmodulation (AM)

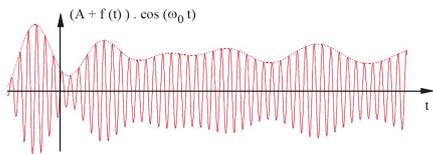
Nutzsignal  $f(t)$



Trägersignal  $\cos(\omega_0 t)$



moduliertes Signal  $(A + f(t)) \cdot \cos(\omega_0 t)$  (um A noch oben verschoben)



## Die Fourier-Transformation

liefert: welche Frequenzen und wie stark?

$$f(t) \xrightarrow{FT} F(\omega) = FT\{f(t)\}$$

Zeitfunktion    Spektrum    Fourier-Transformierte von  $f(t)$

Transformation $F(\omega) = \int_{-\infty}^{\infty} f(t)e^{-j\omega t} dt \quad (j = \sqrt{-1})$	Rücktransformation $f(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} F(\omega)e^{+j\omega t} d\omega$
Real- und Imaginärteil $F(\omega) = R(\omega) + jX(\omega)$	Betrag und Phase $F(\omega) = A(\omega) \cdot e^{j\phi(\omega)}$
$A(\omega) =  F(\omega)  = \sqrt{R(\omega)^2 + X(\omega)^2}$ $e^{j\phi(\omega)}$ Phasenfunktion	Amplitudenfunktion (Betrag) $\phi(\omega) = \arctan \frac{X(\omega)}{R(\omega)}$

### Linearität

$$f(t) = a_1 f_1(t) + a_2 f_2(t) \xrightarrow{FT} F(\omega) = a_1 F_1(\omega) + a_2 F_2(\omega)$$

### Verschiebung

$$f(t - t_0) \xrightarrow{FT} F(\omega)e^{-j\omega t_0}$$

$$f(t)e^{+j\omega_0 t} \xrightarrow{FT} F(\omega - \omega_0)$$

### Zeitdehnung

$$f(at) \xrightarrow{FT} \frac{1}{|a|} F\left(\frac{\omega}{a}\right)$$

(Zeitdauer und Bandbreite eines Signals stehen im umgekehrten Verhältnis)

### Vertauschung

$$f(t) \xrightarrow{FT} F(\omega)$$

$$F(t) \xrightarrow{FT} 2\pi f(-\omega)$$

### Dirac-Impuls und Faltungsoperation

zum bestimmen der Impulsantwort einer Leitung  
enthält alle Frequenzen einer Leitung - Testen welche durchgehen  
Senkrechter Strich als Impuls der Stärke 1 (Fläche 1)

$$\lim_{\tau \rightarrow 0} = A_0 \delta(t - t_0)$$

### Ausblende-Eigenschaft

$$\int_{-\infty}^{\infty} g(t) \cdot A_0 \delta(t - t_0) dt = A_0 g(t_0)$$

### Faltungsoperationen

$$f(t) = [f_1 * f_2](t) = f_1(t) * f_2(t)$$

Berechnung mittels Transformation

$$f(t) = f_1(t) * f_2(t) = \int_{-\infty}^{\infty} f_1(x) \cdot f_2(t - x) dx$$

### Anwendung

Faltung des Signals mit Impulsantwort: man weiß wie das Signal ankommt

## 9.3 Signalverformung durch den Übertragungskanal

### Grundbegriffe

- Eingangssignal  $u_1(t_n)$   
Ausgangssignal  $u_2(t_n)$
- T allgemeiner Operator  $u_2(t_n) = T[u_1(t_n)]$
- t zeitkontinuierlich  $u_2(t) = T[u_1(t)]$
- lineares System  $T[a_1 \cdot u_{11}(t) + a_2 \cdot u_{12}(t)] = a_1 \cdot T[u_{11}(t)] + a_2 \cdot T[u_{12}(t)]$
- zeitinvariantes System  $u_2(t - t_0) = T[u_1(t - t_0)]$
- kausales System  $u_1(t) = 0, t < t_0 \Rightarrow u_2(t) = 0, t < t_0$
- stabiles System  $|u_1(t)| \leq U_{1,max} \Rightarrow |u_2(t)| \leq K \cdot U_{1,max}$   
K systemabhängige Konstante

### Impulsantwort

Dirac-Impuls  $u_1(t) = \delta(t) \rightarrow (T)u_2(t) = T[\delta(t)] = h(t)$  Impulsantwort

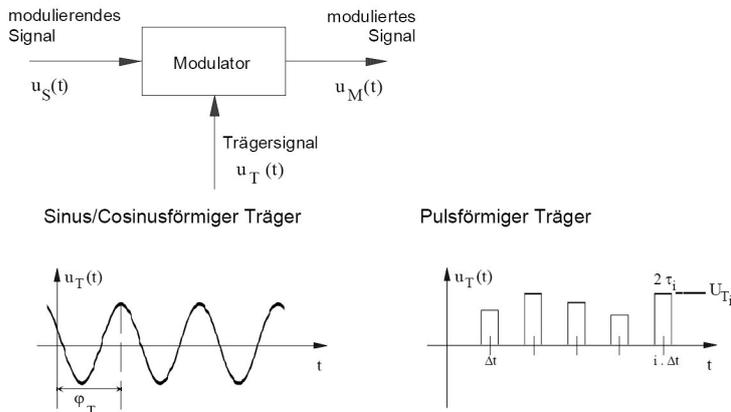
Ein lineares, zeitinvariantes System ist vollständig charakterisiert durch seine Impulsantwort  $h(t)$

Beweis mittels Ausblendeigenschaft und Linearität

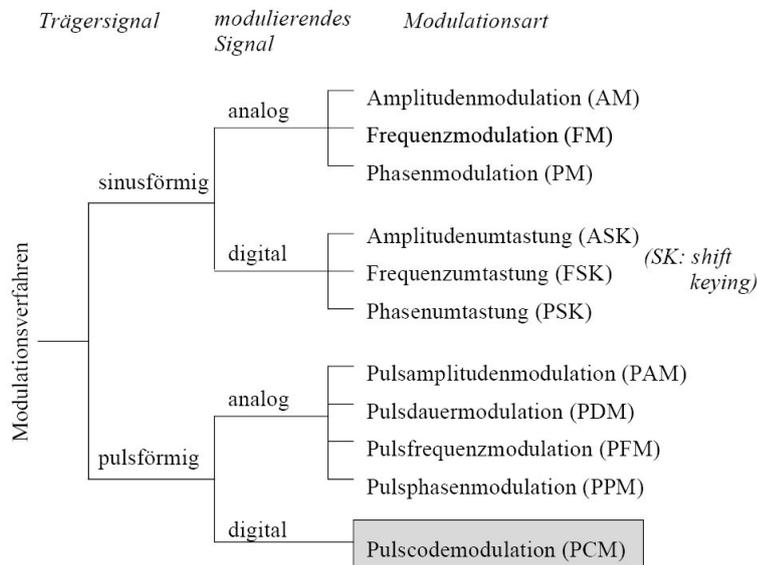
$u_2(t) = u_1(t) * h(t)$ , also  $U_2(\omega) = U_1(\omega) \cdot H(\omega)$  ( $H(\omega)$  heißt Übertragungsfunktion)

## 9.4 Modulation

Anpassung der Signalform an die Übertragungseigenschaften des Übertragungskanals



### Modulationsverfahren



#### Bsp: Amplitudenmodulation

$$u_m(t) = u_s(t) \cdot u_T(t) = (A_0 + u_s(t)) \cos \omega_T(t)$$

Durch Frequenzverschiebung erhält man 2 Seitenbänder (oberes SB, USB)

doppelte Trägerfrequenz wird durch den Tiefpass unterdrückt

## 9.5 Signalabtastung und Abtasttheorem

### Abtasttheorem

Eine durch  $\omega_g$  bandbegrenzte Signal ist durch seine Abtastwerte  $f_n = f(n \frac{\pi}{\omega_g})$  vollständig charakterisiert  
 $f(t)$  lässt sich zurückgewinnen

### Nyquist-Abtastfrequenz

$$\omega_g = 2\pi f_g$$

$$\text{Abtastabstand: } T = \frac{\pi}{\omega_g} = \frac{1}{2f_g} \text{ und } \frac{1}{T} = f_T$$

$$\text{Nyquist-Abtastfrequenz } f_T = 2f_g$$

(doppelt so häufig wie Grenzfrequenz abtasten)

Nyquist-abgetastetes Signal kann vollständig wieder zurückgewonnen werden

Überabtastung  $f_t > 2f_g$

Unterabtastung  $f_t < 2f_g$  (Signalverfälschung wg. Überlappung)

**Tiefpaß** von  $-\omega_g$  bis  $\omega_g$  (Demodulator)

**Hochpaß**

**Bandpaß**

## 9.6 Signalformung und Leitungscodierung

- korrekte Rückgewinnung des digitalen Signals
- schnelle Übertragung

### Impulsformung

mit Impulsantwort wird z.B. eine 1 dargestellt (Manchester-Code)  
 $h(t)$  hat für  $t = 0$  endlichen Wert, sonstige Abtastpunkte: Nullstellen

### Frequency Shift Keying

doppelte Frequenz für 1

### Frequenzmodulation

Steigung (hohe Frequenz)

Fallend (nied. Frequenz)

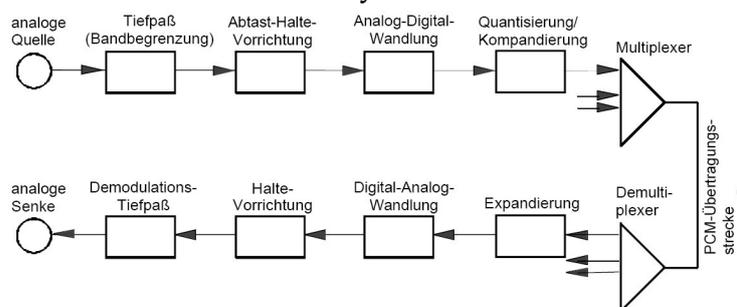
# 10 Komponenten digitaler Übertragungssysteme

## 10.1 Grundfunktionen

### Signalverarbeitung

- Signalwandlung (Modulation, Impulsformung)
- Entzerrung
- Signalfilterung und Verstärkung
- Redundanzverminderung
- Codierung zur Fehlererkennung- und korrektur
- Fehrfachausnutzung (Frequenz-, Zeitmultiplex)
- Signalisierung und Kommunikationssteuerung (Protokolle)

### Puls-Code-Modulationssystem PCM

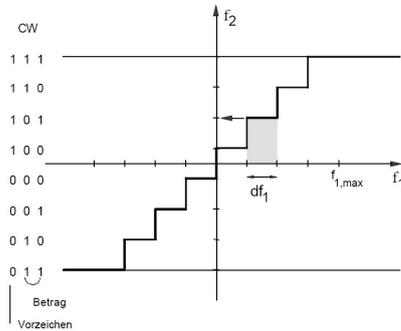


## 10.2 Quantisierung und Analog-Digital-Wandlung

## Quantisierung

Abbildung von wertkontinuierlich zu wertdiskret

### lineare Quantisierung (mit $q$ Quantisierungsstufen)



- Da der Eingangssignalebereich nicht gleichverteilt, sondern um 0 konzentriert ist, ist aus informationstheoretischer Sicht die lineare Quantisierung ungünstig.
- Quantisierungsfehler  $f_\epsilon(t) = f_1(t) - f_2(t)$
- Auftretswahrscheinlichkeit der Eingangsamplituden  $f_1$  wird durch die Amplitudenwahrscheinlichkeitsdichtefunktion  $w(n)$  charakterisiert (Signale im Nullpunkt wahrscheinlicher)
- Quantisierungsgeräuschleistung  $P_Q = \frac{(\delta f_1)^2}{12}$  bei linearer Quantisierung  
Es gilt  $P_Q = \sum_{i=1}^q w(f_{2,i}) \int_{f_{1,i}^{min}}^{f_{1,i}^{max}} (f_1 - f_{2,i})^2 \partial f_1$   
unabhängig von der Amplitudenwahrscheinlichkeitsdichte  
abhängig von der Quantisierungsstufenbreite
- bei gleichwahrscheinlichen Signalwerten  
 $\frac{P_{OUT}}{P_Q} = (q^2 - 1)$
- in Dezibel  $a_Q = 10 \log \frac{P_{OUT}}{P_Q} = 10 \log (q^2 - 1) [dB]$



# 11 Einführung in Kommunikationsnetze

## 11.1 Netzstrukturen

- Maschenstruktur: große Anzahl von Verbindungen
- Sternstruktur: weniger Verbindungswege, mehr Vermittlungsaufwand
- Ringstruktur: (Einfacher Ring, Dualring)
- Busstruktur
- Ethernet: physikalisch: Sternform, Steuerung: busorientierte CSMA-CD

### Wichtige Netzparameter

Ausbreitungsverzögerung (propagation delay)  $\tau = t_p = \frac{l}{v}$

Übertragungszeit  $t_N = \frac{L}{C}$

Busgeschwindigkeit bzw. -kapazität C

Buslänge l

Ausbreitungsgeschwindigkeit v

Paketlänge L

logische Buslänge (bit) :  $a_b = \frac{LC}{v}$  [bit]

logische Buslänge (Pakete) :  $a_N = \frac{LC}{Lv}$  [Pakete]

## 11.2 Beispiel eines Zugriffsprotokolls: Ethernet

### CSMA-CD(Carrier Sense Multiple Acces with Collision Detection)

CS: jede Station hört am Bus mit und fängt erst an zu übertragen wenn Bus frei ist  
Kollision möglich, Auflösung: Contention-Zustand(Kollisionszustand) - JAM-Signal  
CS nur zu bestimmten Zeitpunkten ( $\tau$ )

CS immer

es existiert keine Gleichzeitigkeit im System wegen physikalischer Übertragungsverzögerung

### Back-off-Algorithmus

Auflösung des Contention-Zustands:

nach einer Anzahl von  $k$  Kollisionen verschiebt eine Station den eigenen Sendevorgang um  $1,2,\dots,2^k$  Slots mit Wahrscheinlichkeit  $1/2^k$

- virtuelle Übertragungszeit: tatsächlich benötigte Zeit für Übertragung eines Pakets  
 $T_v = \tau + t_N$  (+ evtl. pro Kollision  $2 * \tau$ )  
Anzahl der Kollisionen geometrisch verteilt
- Versuchswahrscheinlichkeit einer Station  $\frac{1}{n}$   
Grenzwert der Erfolgswahrscheinlichkeit  $v = \lim_{n \rightarrow \infty} (1 - \frac{1}{n})^{n-1} = \frac{1}{e}$
- $E[T_v] = \tau + 2 \cdot \tau \cdot E[X] + t_N = t_N (\frac{\tau}{t_N} \cdot (1 + 2 \cdot \frac{1-\frac{1}{e}}{1}) + 1) = t_N \cdot (1 + a_N \cdot (2e - 1))$
- Maximaler Durchsatz:  $D = \frac{1}{E[T_v]}$
- maximale Busauslastung  $p = D \cdot t_N$

### Ethernet-Technologien

- **10Base2 Ethernet:** Bustopologie, Koaxialkabel
- **10BaseT und 100BaseT:** sternförmig, zentraler Hub(Konzentrator)
- **Gigabit-Ethernet**
- **Hubs:** Repeater der Bitstrom von Eingabeport an die Ausgangsports befördert
- **Bridge:** können Rahmen mit LAN-Zieladressen weiterleiten und filtern
- **Switches:** leistungsstarke Bridges (mehr Schnittstellen)