Zeitschrift: Bulletin de l'Association suisse des électriciens

Herausgeber: Association suisse des électriciens

Band: 59 (1968)

Heft: 25

Artikel: Stand der Technik von Fehlerkorrekturmethoden bei der Datenübertragung

Autor: Ohnsorge, H.

DOI: https://doi.org/10.5169/seals-1057437

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 22.08.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Stand der Technik von Fehlerkorrekturmethoden bei der Datenübertragung

Von *H. Ohnsorge*, Ulm

621.327.8 : 621.3.041.5

Die vorliegende Arbeit bietet einen Überblick, welche Methoden zur Korrektur von Übertragungsfehlern z. Z. bekannt sind und zum Einsatz kommen. Es wird versucht, die derzeitigen Probleme auf diesem Gebiet und die Bemühungen um eine Weiterentwicklung herauszuarbeiten. Bei der Behandlung der Verfahren zur direkten Fehlerkorrektur durch redundante Codes ist u. a. ein System für Ähnlichkeitsdecodierung beschrieben, das nach Wissen des Autors bisher nicht bekannt war. Die Systeme mit Fehlerkorrektur durch Wiederholung gestörter Information befinden sich bereits im Einsatz und werden daher nur kurz gestreift. Allein die Nützlichkeit der Kombinationen von Code und Stördetektoren zur Fehlererkennung ist noch nicht hinreichend untersucht worden. Die ersten Ergebnisse der diesbezüglichen Arbeiten werden wiedergegeben.

Le présent exposé fournit un aperçu des méthodes actuellement connues et appliquées à la correction des fautes de transmission. L'auteur tente de dégager les problèmes suscités à présent par ce domaine et les efforts tentés en vue d'un développement ultérieur. Lors du traitement des procédés de correction directe au moyen de codes redondants, il décrit entre autres également un système de codage analogique, jusqu'à présent inédit à son point de vue. Les systèmes de correction par répétition de l'information perturbée sont déjà actuellement appliqués, et ne sont de ce fait qu'esquissés. Toutefois l'utilité des combinaisons de codes et de détecteurs de perturbations n'a pas encore fait l'objet d'études suffisantes. L'exposé fournit les premiers résultats acquis lors de ces recherches.

1. Einleitung

Seit dem Erscheinen der Arbeiten von *Shannon* [1][1]) und *Hamming* [2] arbeitet man intensiv in vielen Instituten und Laboratorien an Methoden zur gesicherten Datenübertragung. *Shannon* hat die Grenzen des Erreichbaren in seiner fundamentalen Arbeit über Informationstheorie abgesteckt. Ausschlaggebend für die Datensicherung ist der Shannonsche Satz, dass über einen Kanal mit statistisch unabhängigen Übertragungsfehlern durch redundante Codierung die Fehlerwahrscheinlichkeit auf Null reduziert werden kann, wenn die Entropie der Quelle kleiner oder im Grenzfall gleich der Kanalkapazität ist. Die Fehlerwahrscheinlichkeit Null erreicht man aber erst bei unendlich langen Codewörtern, die praktisch natürlich nicht realisiert werden können. Der Aufwand — speziell für die Decodierung — steigt mit zunehmender Codewortlänge sogar so stark, dass man bei den bisher bekannten Verfahren nur mit relativ kurzen Codewörtern bzw. Blöcken arbeiten kann. Die derzeitigen Arbeiten sind daher in erster Linie auf das Ziel gerichtet, Methoden zu finden, die mit möglichst geringem Geräteaufwand die geforderte Restfehlerwahrscheinlichkeit gewährleisten.

In der vorliegenden Arbeit soll ein Überblick gegeben werden, welche Ergebnisse diese Bemühungen bisher erbracht haben und in welche Richtung die augenblicklichen Arbeiten tendieren.

2. Methoden zur gesicherten Datenübertragung

Für die Übertragung von Daten steht z. Z. das Fernschreib- und Fernsprechnetz zur Verfügung. Bei ungesicherter Übertragung bietet das Fernschreibnetz (bei stark gestörten Verbindungen) eine mittlere Fehlerwahrscheinlichkeit p von:

$$p_{\text{Fernschr.}} \approx 10^{-4} \ldots 10^{-6}$$

und das Fernsprechnetz

$$p_{\text{Fernsprech}} \approx 10^{-2} \ldots 10^{-4}$$

Ungesicherte Übertragung heisst: die Zeichen der Quelle werden direkt über den Modulator (Mo) auf den Übertragungskanal gegeben und nach der Demodulation (Dem) unbesehen an die Senke geliefert.

Die Fehlerwahrscheinlichkeit wird durch Datensicherungseinrichtungen (DSE) herabgesetzt (Fig. 1), und man fordert im allgemeinen bei gesicherter Übertragung eine Restfehlerwahrscheinlichkeit von kleiner 10^{-8}. Die DSE können z. B. Einrichtungen zur Fehlerkorrektur durch redundante Codes sein. Für Datenübertragung im Fernsprechnetz stellen die Postverwaltungen neben dem Hauptkanal (HK) für Rückmeldungen einen Schmalband-Rückkanal (RK) zur Verfügung. Damit ist der Einsatz von Systemen mit Entscheidungsrückmeldung und Korrektur durch Wiederholung gestörter Information möglich.

Die Verfahren zur gesicherten Datenübertragung können bezüglich ihrer Wirksamkeit nur beurteilt werden, wenn man die Stör- und Fehlerstruktur der verwendeten Übertragungskanäle genau kennt. Aus diesem Grunde sind von den Postverwaltungen und von der Industrie umfangreiche Messungen durchgeführt worden. Ergebnisse dieser Untersuchungen findet man u. a. in [3; 4; 5].

Wenigstens erwähnt seien die Primitivmethoden zur Datensicherung und zwar:
die *Mehrfachübertragung* jedes Zeichens und Fehlererkennung durch Vergleich der Empfangssignale und das *Echoverfahren*, bei dem man jedes übertragene Zeichen wieder zurück zum Sender schickt und auf der Sendeseite durch Vergleich feststellt, ob eine Störung stattgefunden hat.

Behandelt sind diese Verfahren in den Literaturstellen [6] und [7]. Der Aufwand an Redundanz ist hiebei im Vergleich zu den im Folgenden behandelten Methoden so hoch, dass ein Einsatz nur in Sonderfällen sinnvoll ist.

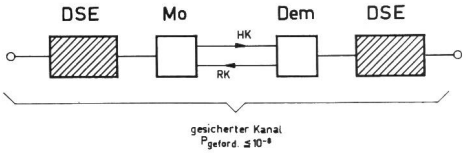


Fig. 1
System zur gesicherten Datenübertragung
Bezeichnungen siehe im Text

[1]) Siehe Literatur am Schluss des Aufsatzes.

3. Fehlerkorrektur durch redundante Codes

Ein redundanter Code lässt sich z. B. bilden, indem man mögliche Sendezeichen als unzulässig erklärt. Entsteht durch Verfälschung auf dem Übertragungskanal ein unzulässiges Zeichen, dann erkennt dies der Empfänger. Sucht er das zulässige Zeichen heraus, das dem empfangenen Zeichen am ähnlichsten ist und betrachtet dieses als Empfangszeichen, dann hat er eine Fehlerkorrektur nach der Ähnlichkeitsdecodierung bzw. «maximum likely-hood-detection» durchgeführt. Die Bildung von Codewörtern, d. h. von zulässigen Sendezeichen, erfolgt heute in erster Linie durch lineare systematische Codierung [8], daher sei dieses Verfahren etwas eingehender erläutert.

3.1 Lineare systematische Codes

Eine Quelle sende die Zeichen $x_1, x_2, x_3, \ldots$ aus. Zur Vereinfachung sei angenommen, dass die Alphabetbuchstaben der Quelle binär codiert sind, also nur die Zeichen 0 oder 1 ausgesendet werden. Leitet man aus jeweils K Informationszeichen durch lineare Verknüpfung m Prüfzeichen ab und überträgt diese als Redundanz mit den Informationszeichen, dann hat man einen linearen systematischen Code gebildet. Am universellsten sind diese Codes durch die Matrixdarstellung [8; 9] zu beschreiben. Die jeweils K Informationszeichen werden als einspaltige Matrix $[X]^+$ geschrieben. Durch Multiplikation mit der sog. Codiermatrix $[A]$ entsteht die Prüfzeichenmatrix $[Y]$ entsprechend Gl. (1):

$$\begin{bmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mk} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix}^* = \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} \tag{1}$$

oder vereinfacht geschrieben:

$$[A] \cdot [X]^+ = [Y] \tag{2}$$

Es sei $Y_i = X_{k+i}$ und Gl. (2) sei verwandelt in ein homogenes Gleichungssystem, dann wird $[A]$ um die Einheitsmatrix $[I]$ ergänzt und man erhält:

$$[A, I] \cdot [x, y] = [B] \cdot [K] = 0 \tag{3}$$

$[X]$ ist nun das zu sendende Codewort. Die Addition erfolgt modulo 2 im Binärfall bzw. modulo q, wenn die Quelle q verschiedene Symbole ausgibt. Im Binärfall sind die Komponenten:

$$a_{ij} \quad \text{bzw.} \quad b_{ij} \begin{cases} 0 \\ \text{oder} \\ 1 \end{cases}$$

Bei der Übertragung entstehen Fehler; man kann sich die Fehler durch Überlagerung eines Fehlerwortes $[X]_f$ über das Codewort $[X]$ vorstellen, so dass auf der Empfangsseite das fehlerhafte Wort:

$$[X]_e = [X] + [X]_f$$

eintrifft. Bildet man nun:

$$[B] \cdot [X]_e = \underbrace{[B] \cdot [X]}_{0} + [B] \cdot [X]_f = [F]$$

so erhält man eine einspaltige Fehlermatrix

$$[F] = [B] \cdot [X]_f \tag{4}$$

die nur von $[X]_f$ abhängt. Nun gibt es bedauerlicherweise bei $n = k + m$ insgesamt 2^n Fehlerwörter, aber nur 2^m Fehlermatrizen, denn ein Codewort hat n und eine Fehlermatrix nur m Komponenten. Es ist also keine umkehrbar eindeutige Zuordnung zwischen $[F]$ und $[X]_f$ möglich. Andernfalls könnte man alle Übertragungsfehler richtig korrigieren, indem man durch $[F]$ das Fehlerwort $[X]_f$ bestimmt und:

$$[X]_e + [X]_f = [X] \tag{5}$$

bildet. Addition und Subtraktion sind in der Algebra der ganzen Zahlen modulo 2 gleichbedeutend, daher kann in Gl. (5) plus verwendet werden. Soll ein Code alle Fehlermuster mit 1 bis e Binärfehlern im Codewort korrigieren können, dann muss die Zahl $Z = 2^m - 1$ der Fehlermatrizen, die ungleich [0] sind, grösser oder gleich $\sum_{i=1}^{e} \binom{n}{i}$ sein, denn in einem n-Tupel gibt es $\binom{n}{j}$ Konfigurationen mit i Einsen. Die Bedingung:

$$2^m - 1 \geqq \sum_{i=1}^{e} \binom{n}{i} \tag{6}$$

ist die bekannte Hamminggrenze, aus der hervorgeht, wieviel Prüfzeichen ein Code mindestens enthalten muss, um e Fehler mit Sicherheit korrigieren zu können.

In Fig. 2 ist die Realisierung eines Fehlerkorrektursystems gezeichnet, das nach Gl. (5) arbeitet: In ein Register wird das empfangene Wort $[X]_e$ eingegeben. Die Nachbildung der $[B]$-Matrix durch modulo-2-Addierer erzeugt mit $[X]_e$ nach Gl. (4) die Matrix $[F]$, nachdem das vollständige Empfangswort im Register steht. Die Registerstufen sind bistabile Elemente, also Stufen, die selbsttätig modulo 2 addieren. Der Fehlerwortgenerator bildet nun der Reihe nach die korrigierbaren Fehlerwörter und überlagert sie dem Empfangswort. Im Register wird also

1. $[X]_e + [X]_{f1}$
2. $[X]_e + [X]_{f1} + [X]_{f1} = [X]_e$
3. $[X]_e + [X]_{f2}$
4. $[X]_e + [X]_{f2} + [X]_{f2} = [X]_e$

   usw.

erzeugt, bis $[B] \cdot ([X]_e + [X]_{fj}) = [0]$ entsteht. In diesem Falle ist $[X]_e + [X]_{fj} = [X]$ das korrigierte Codewort, das an die Senke ausgegeben wird. Die Reihenfolge der Fehlerwörter $[X]_f$ wählt man so, dass zuerst das wahrscheinlichste Fehlerwort erzeugt wird, dann das zweitwahrscheinlichste usw.; damit ist sichergestellt, dass mit der kleinsten Anzahl von Schritten die Korrektur durchgeführt wird. Sind bei einem e Fehler korrigierenden Code mehr als e Binärfehler im Empfangswort, dann erfolgt die Korrektur falsch. Zur Bildung der Prüfzeichenmatrix $[Y]$ kann in entsprechender Weise die Nachbildung der Matrix $[A]$ durch Mod-2-Addierer verwendet werden.

Das hier beschriebene Verfahren arbeitet mit Ähnlichkeitsdecodierung, d. h. nach der optimalen Methode bei statistisch unabhängigen Fehlern. Es erfordert im Mittel wesentlich weniger als 2^m Vergleiche. Ursprünglich hatte man für «maximum likelyhood-detection» 2^k Vergleiche für notwendig gehalten, da man von der Vorstellung ausgegangen war, man müsse das empfangene Wort $[X]_e$ mit allen 2^k zulässigen Codewörtern vergleichen, um das dem Empfangswort ähnlichste

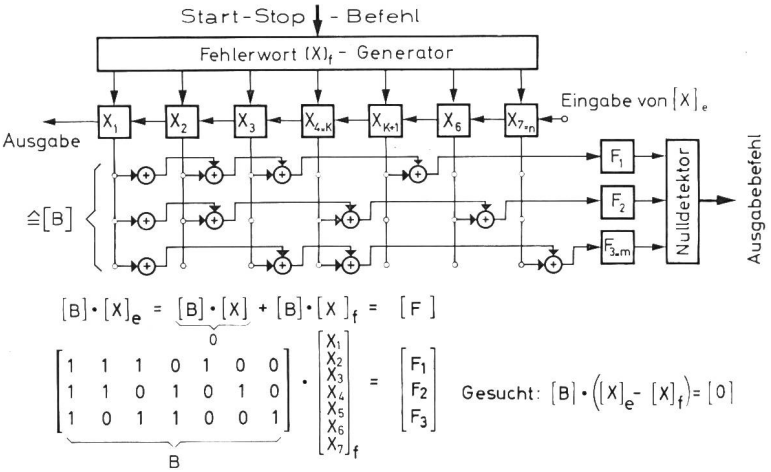


Fig. 2
Fehlerkorrektur-System
Bezeichnungen siehe im Text

zu ermitteln. Das Verfahren nach Fig. 2 erfordert einen technischen Aufwand, der proportional zu $n \cdot m$ steigt.

Für eine Reihe von linearen systematischen Codes lässt sich die Codierung und Fehlererkennung einfacher mit Hilfe von rückgekoppelten Schieberegistern realisieren. Derartige Codes werden mit Hilfe der *Polynomdarstellung* [10; 11] behandelt. Betrachtet man die Informationszeichen $(x_1\, x_2 \ldots x_k)$ als Koeffizienten eines Polynoms:

$$f^*(X) = x_1 X^{k-1} + x_2 X^{k-2} \ldots + x_k X^0$$

dann kann man die Prüfzeichen bestimmen, indem:

$$\frac{X^m \cdot f^*(X)}{g(X)} = q^*(X) + \frac{r(X)}{g(X)} \qquad (7)$$

gebildet wird und die Koeffizienten des Restpolynoms $r(x)$ im Anschluss an $(x_1\, x_2 \ldots x_k)$ als Prüfzeichen gesendet werden. Ein Codewort hat dann als Polynom geschrieben die Form:

$$X^m \cdot f^*(X) - r(X) = q^*(X) \cdot g(X) = C(X) \qquad (8)$$

Das Polynom $g(X)$ ist vom Grade m und wird Generatorpolynom des Codes genannt. Die Übertragungsfehler in einem Codewort können nun ebenfalls als ein Polynom $f(X)$ aufgefasst werden, so dass am Empfangsort das Wort:

$$E(X) = C(X) + f(X)$$

eintrifft. Bildet man nun:

$$\frac{E(X)}{g(x)} = \frac{C(X) + f(X)}{g(x)} = \frac{q^*(X) \cdot g(X)}{g(X)} + \frac{f(X)}{g(X)} =$$

$$= q^*(X) + q(X) + \frac{F(X)}{g(X)} \qquad (9)$$

dann ist das Restpolynom $F(X)$ wieder nur von dem Fehlerwort $f(X)$ abhängig und kann zur Bestimmung von diesem benutzt werden. $F(X) = 0$ bedeutet, dass die Übertragung des betreffenden Codewortes fehlerfrei war oder ein nicht erkennbares Fehlermuster aufgetreten ist. Nicht erkennbar durch lineare systematische Codes sind alle Fehlermuster, die gleich einem Codewort sind, wie man aus Gl. (4) und (8) erkennt.

Das Generatorpolynom hat die Form:

$$g(X) = X^m + g_1 X^{m-1} \ldots g_{m-1} X^1 + 1$$

mit $g_i = 0$ oder 1. Ein Register nach Fig. 3, bei dem die Rückführungen durch die Koeffizienten g_i bestimmt sind, führt in k-Schritten — das heisst nacheinander bei Eingabe der k-Informationszeichen — die Operation gemäss Gl. (7) durch.

Die Koeffizienten r_i des Restpolynoms $r(X)$ stehen nach dem k-ten Schritt im Register und könnnen als Redundanz den k Informationszeichen hinzugefügt werden. Für den Decodiervorgang nach Gl. (9) wird das gleiche Register verwendet. Nach Eingabe der n Empfangszeichen von $E(x)$ enthält das Register die Koeffizienten von $F(X)$. Ein Nulldetektor (Fig. 3) prüft, ob alle Registerstufen auf 0 stehen, d. h. ob $F(X) = 0$ ist; andernfalls liegt ein erkennbarer Fehler vor. Die Eigenschaften von rückgekoppelten Schieberegistern wurden zuerst von *Huffmann* [10] eingehend beschrieben. Teilt $g(X)$ das Polynom $X^n - 1$ ohne Rest, dann erzeugt $g(X)$ einen zyklischen Code. *Bose* und *Chandhuri* [8] haben für $g(X)$ von zyklischen Codes Konstruktionsvorschriften gegeben, so dass der Code eine bestimmte Anzahl von Fehlern sicher korrigieren kann. *Fire* [8] hat für $g(X)$ von zyklischen Codes Vorschriften gegeben, so dass sich der betreffende Code besonders für die Korrektur von gebündelten Fehlern eignet.

Bei vorgegebener Redundanz sinkt die Restfehlerwahrscheinlichkeit mit wachsender Blocklänge, anderseits steigt aber der Zeit- und Schaltungsaufwand für die Fehlerkorrektur durch linearen systematischen Codes mit zunehmender Blocklänge n ausserordentlich stark an, so dass man bei ca. 20 % Redundanz kaum mit wesentlich grösseren Blocklängen als $n = 100$ arbeiten kann. Aus diesem Grunde wurde von *Wotzencraft* und *Reiffen* [12] eine andere Methode entwickelt, deren Prinzip im folgenden Kapitel erläutert wird.

3.2 Convolution Encoding, Sequential Decoding

Das Verfahren «convolution encoding, sequential decoding» bietet zwar z. T. keine optimale Ausnutzung der Redundanz, wie dies z. B. mit dem Verfahren nach Fig. 2 möglich ist, dafür erfordert es bei gleicher Restfehlerwahrscheinlichkeit weniger Aufwand an Zeit und Schaltmitteln.

Convolution encoding arbeitet mit einer Binärfolge als sogenanntem Generator (Fig. 4a). Jedem Informationszeichen wird mindestens ein Prüfzeichen hinzugefügt. Die Ableitung der Prüfzeichen geschieht durch den Generator, wie dies an nachfolgendem einfachen Beispiel mit zwei Prüfzeichen pro Informationszeichen gezeigt wird. Der Generator habe die Form 1 1 1 0 1 0 0 0 1. Unter jede «1» in der Informationszeichenfolge schreibt man den Generator entsprechend Fig. 4a.

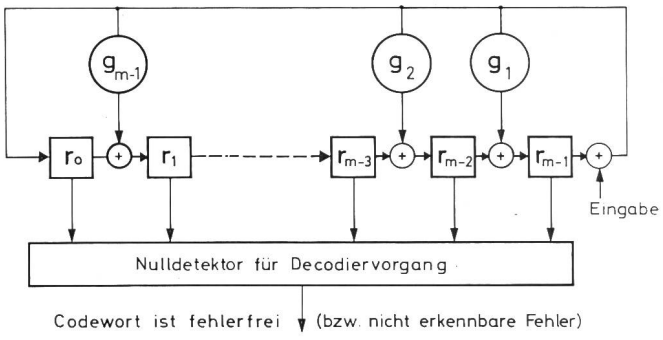
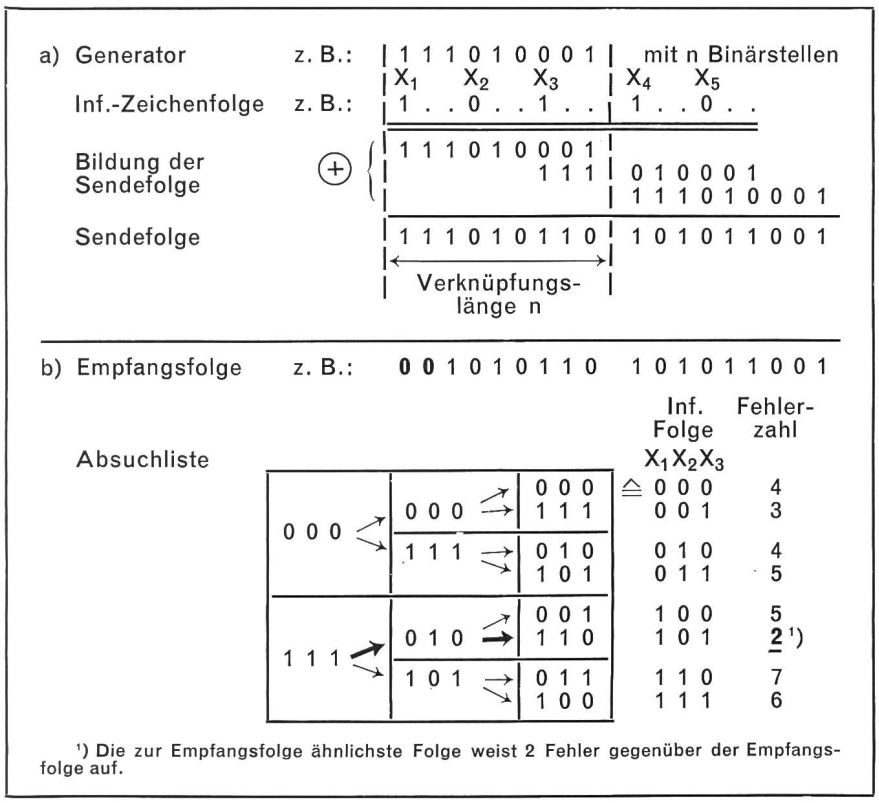


Fig. 3
Codier-Decodier-Register
Codierung = Prüfzeichenbildung; Decodierung = Fehlererkennung



[1]) Die zur Empfangsfolge ähnlichste Folge weist 2 Fehler gegenüber der Empfangsfolge auf.

Fig. 4
Convolution Encoding (a) und Sequential Decoding (b)

Die mod-2-Summe der Generatorfolgen wird als Sendefolge übertragen. Die sequentielle Decodierung geschieht mit Hilfe der Absuchliste (Fig. 4b), in der die möglichen $(1 + i)$-Tupel so geordnet sind, dass sich die Komponenten in den Spalten möglichst stark voneinander unterscheiden; i ist die Zahl der Prüfzeichen pro Informationszeichen. Die Absuchliste enthält als Codebaum alle möglichen Binärkonfigurationen der Verknüpfungslänge n. Man sucht nun nach Empfang der ersten n Binärzeichen in der Absuchliste die Folge von $(1 + i)$-Tupeln aus, die der Empfangsfolge am ähnlichsten ist, dabei sind nur die durch die Pfeile angedeuteten Binärfolgen zulässig. In der in Fig. 4b angenommenen Empfangsfolge mit zwei Fehlern hat die durch dicke Pfeile angedeutete Folge in der Absuchliste die grösste Ähnlichkeit. Alle anderen Folgen weisen mehr Fehler gegenüber der Empfangsfolge auf. Die ersten drei Informationszeichen haben nach diesem Vergleich mit grösster Wahrscheinlichkeit die Form 1 0 1. Der Decodierer trifft aber nur für das erste Informationszeichen die Entscheidung $X_1 = 1$. Nun wird von den ersten n Binärzeichen der Empfangsfolge die Generatorfolge abgezogen. Beginnend mit dem zweiten Informationszeichen wird dann mit dem verbleibenden Rest der weiteren n Empfangszeichen wieder der Vergleich in der Absuchliste durchgeführt und daraufhin X_2 entschieden usw. Die Decodierung bzw. Fehlerkorrektur erfolgt also Zeichen für Zeichen im Gegensatz zu den Blockcodes. Sobald ein Binärzeichen falsch decodiert wird, pflanzt sich der Fehler u. U. bis zum Ende der Sendung fort.

Der Schaltungsaufwand steigt bei diesem Verfahren etwa proportional mit der Generatorlänge n. Die Restfehlerwahrscheinlichkeit sinkt nach der Beziehung:

$$p_{\text{Brest.}} < a \cdot e^{-bn}$$

a; b sind Konstanten.

Man benötigt etwa n Rechenschritte für die Decodierung von einem Binärzeichen. Das hier beschriebene Verfahren erfordert mindestens 50 % Redundanz. Varianten dieser sequentiellen Verfahren wurden von *Gallager* [13] und *Massey* [14] beschrieben. Man kann z. B. bei der Codierung mit mehreren Generatorfolgen arbeiten; damit lässt sich die Redundanz vermindern, aber der Schaltungsaufwand wird dann grösser.

Als Konkurrenz zu dem Verfahren von *Wotzencraft* und *Reiffen* sind die Verfahren der *stufenweisen Codierung* und *Decodierung* bekannt geworden. Eine eingehende Untersuchung dieser Verfahren liegt von *Forney* [15] vor.

3.3 Stufenweise Codierung und Decodierung

Eine interessante Methode der stufenweisen Codierung hat vor kurzem *Ziv* [16] veröffentlicht. Anhand dieser Arbeit soll das Wesen dieser Datensicherungsverfahren kurz erläutert werden. Die Codierung erfolgt bei *Ziv* in drei Stufen:

1. Stufe: Jeweils k_1 Informationszeichen werden mit Hilfe einer Matrix $[A]_1$ zu Codewörtern der Länge n_1 codiert (Fig. 5).

2. Stufe: Aus k_1 derartigen Codewörtern $[X]_{i1}$ werden die Spalten einer Matrix der Form:

$$\begin{bmatrix} X_{11} & X_{12} & \cdots & X_{1k_1} \\ X_{21} & X_{22} & \cdots & X_{2k_1} \\ \vdots & & & \vdots \\ X_{n_1 1} & X_{n_1 2} & \cdots & X_{n_1 k_1} \end{bmatrix}$$

1. Stufe: $[A]_1 \cdot [X]^*_{i1} = [Y]_i \longrightarrow [X, Y]_{i1} = [X]_{i1}$

$K_1 + m_1 = n_1$

2. Stufe: $[X]_{11}\ [X]_{21} \quad [X]_{K_1 1}$

$$\begin{bmatrix} X_{11} & X_{12} & \cdots & X_{1K_1} \\ X_{21} & X_{22} & \cdots & X_{2K_1} \\ \vdots & & & \vdots \\ X_{n_1 2} & X_{n_1 2} & \cdots & X_{n_1 K_1} \end{bmatrix} \begin{matrix} \leftarrow [X]^*_{12} \\ \leftarrow [X]^*_{22} \\ \\ \leftarrow [X]^*_{n_1 2} \end{matrix}$$

$[A]_2 \cdot [X]^*_{i2} = [Y]_{i2} \longrightarrow [X, Y]_{i2} = [X]_{i2}$

$K + m_2 = n_2$

3. Stufe: $[X]_{12} = [\underbrace{X_1\, X_2 \cdots X_\nu}_{f_1(X)}\ \underbrace{X_{\nu+1} \cdots X_{2\nu}}_{f_2(X)} \cdots]; [X]_{22} = [\underbrace{X_1\, X_2 \cdots X_\nu}_{f_{\frac{n_2}{\nu}+1}(X)}\ X_{\nu+1} \cdots$

Fig. 5
Stufenweise Codierung

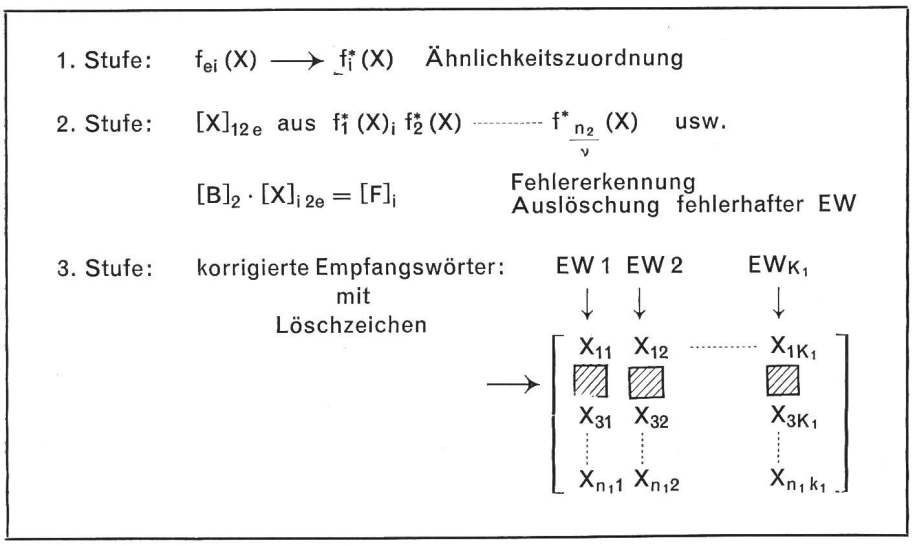


Fig. 6
Stufenweise Decodierung
Nur Korrektur der Löschzeichen in EW_i

gebildet. Die Reihen dieser Matrix werden als Informationszeichen eines zweiten linearen systematischen Codes der Blocklänge n_2 aufgefasst, den man mit der Matrix $[A]_2$ bildet. *Ziv* wählt $n_1 = n_2$.

3. Stufe: Die Blöcke $[X]_{i2}$ des zweiten Codierers werden durch einen dritten Codierer in Abschnitte der Länge ν unterteilt, wobei ν die Zahl n_2 teilt. Jedem derartigen Abschnitt ordnet der dritte Codierer ein redundantes Sendezeichen $f_i(X)$ (*Ziv* nennt es eine «Wellenform») zu. Wir können zur Vereinfachung aber annehmen, dass die ν-Zeichen wieder als Informationszeichen eines Codes der Länge n_3 aufgefasst werden.

Decodiert wird gleichfalls in drei Stufen (Fig. 6):

1. Stufe: Die Empfangswörter $f_{ei}(X)$ der Länge n_3, die den gesendeten Wörtern $f_i(X)$ entsprechen, werden z. B. entsprechend Fig. 2 decodiert, also nach der Methode der grössten Ähnlichkeit korrigiert; man erhält als korrigierte Empfangswörter $f_1^*(X)$; $f_2^*(X)$ usw.

2. Stufe: Der erste Codierer liefert allein die korrigierten ν-Informationszeichen des Codes der Länge n_3 an den zweiten Decodierer. Dieser führt anhand des Codes mit der Länge n_2 z. B. entsprechend Fig. 2 oder 3 eine Fehlererkennung durch. Fehlerhafte Empfangswörter EW werden gelöscht, und es entsteht eine Matrix entsprechend der zweiten Codierstufe, die «Löschzeichen» enthält.

3. Stufe: Die so gebildeten Empfangswörter EW_i der Länge n_1 mit Schmierzeichen (bzw. Löschzeichen) werden korrigiert, indem man allein die Schmierzeichen durch Binärzeichen ersetzt, so dass die Fehlermatrix $[F] = 0$ wird.

Der Aufwand dieses Verfahrens steigt mit n_1^{α}. α ist endlich, wenn die Übertragungsrate R klein gegenüber der Kanalkapazität C ist. Als Grenzwert gilt $\alpha \to 2$ bei $R \to 0$. Die Zahl der Rechenschritte ist proportional zu n_1^2. Für die Restfehlerwahrscheinlichkeit wird von *Ziv* die Grenze:

$$P_{\text{Brest.}} < (e + n_1) \cdot 2^{-[1-(R/C)^{1/3}]\,n_1}$$

bei $n_1 = n_2$ und $R < C$ angegeben. Hiebei ist e nur bestimmt durch:

$$e > \left(1 + \frac{1}{n_1}\right)^{n_1}$$

Vergleichend kann gesagt werden: Von den bekannten Verfahren nutzen die linearen systematischen Codes die Redundanz am günstigsten aus. Sie erfordern aber den grössten Schaltungs- und Zeitaufwand für die Fehlerkorrektur.

Den kleinsten Aufwand an Zeit und Schaltmitteln braucht man für «convolution encoding» und «sequentiell decoding». Dieses Verfahren arbeitet aber mit der grössten Redundanz und besitzt den Nachteil der Fehlerfortpflanzung.

Zwischen diesen Verfahren liegt die stufenweise Codierung und Decodierung, für die viele Varianten denkbar sind. Es hat den Anschein, als müsste man bei vorgegebener Restfehlerwahrscheinlichkeit die Verminderung des Zeit- und Schaltungsaufwandes stets durch Vergrösserung der Redundanz erkaufen.

4. Systeme mit Entscheidungsrückmeldung und Fehlerkorrektur durch Wiederholung

Die Fehlerstruktur bei Datenübertragung auf Fernsprechkanälen macht den Einsatz von redundanten Codes zur Fehlerkorrektur sinnlos, da hier die Wiederholverfahren bei gleichem Aufwand und gleicher Restfehlerwahrscheinlichkeit mit höherer effektiver Übertragungsrate V_{eff} arbeiten. V_{eff} ist das Verhältnis der mittleren Geschwindigkeit v_s, mit der die Datensenke Binärzeichen erhält zur Geschwindigkeit v_k, mit der der Fernsprechkanal Binärzeichen überträgt, also:

$$V_{\text{eff}} = \frac{v_s}{v_k}$$

Der redundante Code wird hiebei nur zur Fehlererkennung z. B. entsprechend Fig. 2 verwendet. Fehler können aber mit einer hohen Wahrscheinlichkeit auch durch Störungsdetektoren erkannt werden.

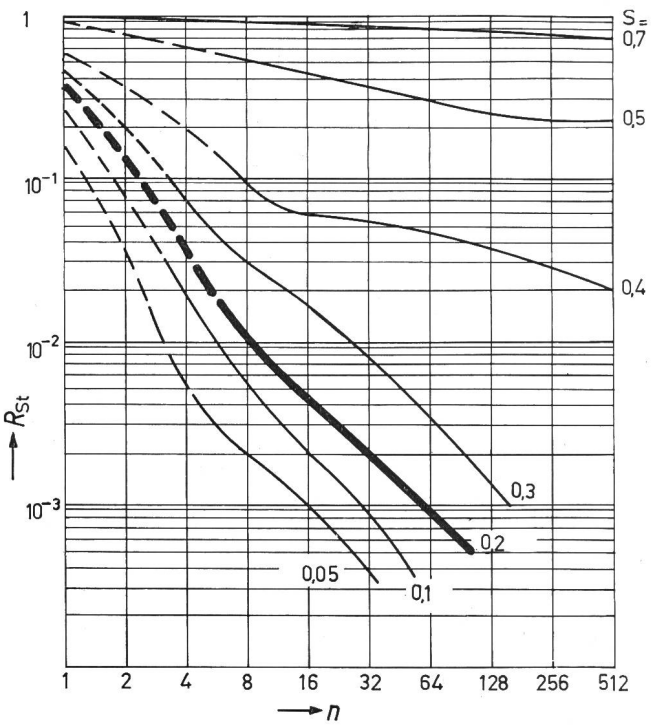


Fig. 7
Fehler-Reduktionsfaktor eines Stördetektors
Reduktionsfaktor R_{St} der Blockfehlerwahrscheinlichkeit als Funktion der Blocklänge n bei konstantem Schwellenabstand S und Störungen von Fernsprechkanälen für den Amplitudentoleranzdetektor
Binäre Frequenzumtastung mit 1200 bit/s;
Empfangspegel $a_0 = -30$ dBmo

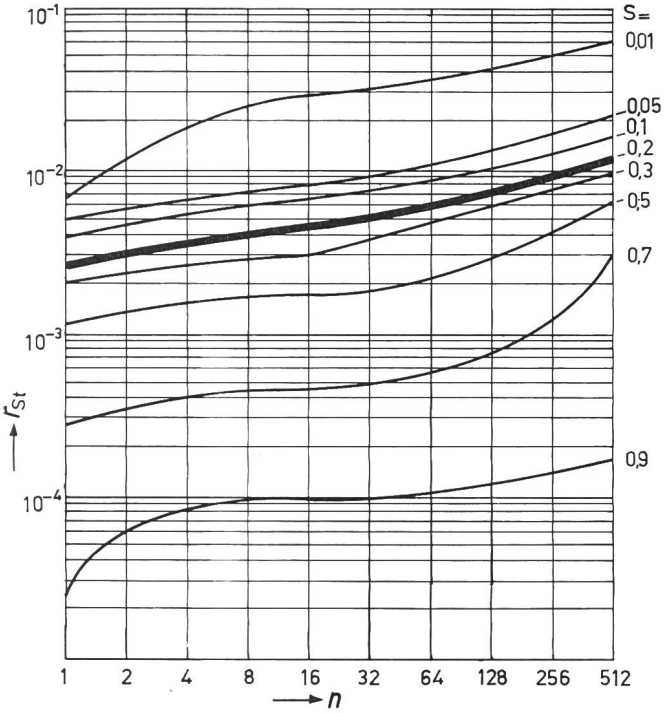


Fig. 8
Redundanz bei blockweiser Störanzeige
Redundanz r_{St} infolge der Störanzeige als Funktion der Blocklänge n bei konstantem Schwellenabstand S und Störungen von Fernsprechkanälen für den Amplitudentoleranzdetektor
Binäre Frequenzumtastung mit 1200 bit/s;
Empfangspegel a_0 = — 30 dBmo

4.1 Störungsdetektoren

Störungsdetektoren vergleichen die analogen Empfangssignale mit den zulässigen Sollsignalen. Überschreiten die Abweichungen der Empfangssignale von ihrer Sollform vorgebbare Grenzen, dann gibt der Detektor Störalarm und eine Wiederholung wird eingeleitet. Für Störungsdetektoren sind eine Vielfalt von Ausführungsformen denkbar, in der zu diesem Punkt angegebenen Literatur [17...19] findet man eine Reihe von Realisierungsmöglichkeiten. *Marko* hat den sog. Amplitudentoleranzdetektor vorgeschlagen, der vor kurzem in modifizierter Form auch im CCITT zur Normung empfohlen wurde. Dieser Stördetektor zeichnet sich durch Einfachheit und gute Leistungsfähigkeit aus. Man prüft damit, ob die Amplituden der Binärsignale nach der Demodulation den Wert $\pm S$, der auf die Sollamplitude bezogen ist, überschreiten. Führt man die Wiederholentscheidung jeweils für Blöcke von n Binärzeichen resultierend durch, dann bleiben fehlerhafte Blöcke mit der Wahrscheinlichkeit:

$$p_{\text{Brest.}} = p_{\text{B}}\, R_{\text{st}}$$

unerkannt (p_{B} ist die Wahrscheinlichkeit, dass ein Block Fehler enthält; $R_{\text{st}}(n, S)$ ist in Fig. 7 gezeigt. Störanzeige kann mit gewisser Wahrscheinlichkeit aber auch erfolgen, obgleich der Empfänger die Zeichen noch richtig interpretiert. Die hiedurch entstehende unnütze Wiederholung bedeutet Redundanz r_{st}. In Fig. 8 ist $r_{\text{st}}(n, S)$ wiedergegeben.

Ein interessanter Effekt zeigte sich bei der Untersuchung von *Kombinationen von Code + Störungsdetektor*. Reduziert ein Stördetektor die Blockfehlerwahrscheinlichkeit p_{B} um den Faktor R_{st} und ein Code entsprechend um den Faktor R_{c}, so dass:

$$p_{\text{Brest}} = p_{\text{B}}\, R_{\text{c}}$$

ist, dann wird bei kombiniertem Einsatz von Code + Stördetektor:

$$p_{\text{Brest}} < p_{\text{B}}\, R_{\text{c}}\, R_{\text{st}}$$

d. h. der resultierende Reduktionsfaktor R_{stc} ist kleiner als das Produkt der Einzelreduktionsfaktoren, also:

$$R_{\text{stc}} < R_{\text{c}}\, R_{\text{st}}$$

Eine theoretische Begründung für diesen Effekt ist in [20] gegeben. Das Ergebnis einer Messung zeigt Fig. 9.

Der kombinierte Einsatz von Code + Stördetektor zur Fehlererkennung dürfte die wirksamste Fehlererkennungsmethode sein.

4.2 Systemorganisation

Für Systeme mit Wiederholung gestörter Information sind viele Systemorganisationen denkbar. Man kann aber diese Organisationen in drei Gruppen mit charakteristischen Unterschieden einteilen, wie dies anhand der Speicherorganisation in Fig. 10 geschehen ist. Bei *Semiduplexsystemen* sendet man einen Block, wartet, bis die Quittung dafür eintrifft, und sendet dann den nächsten Block, bzw. man wiederholt den Block, wenn dies angefordert wird. Das Warten auf die Quittung bedeutet Verlustzeit bzw. Redundanz. Diese Verlustzeit vermeiden *Wechselspeichersysteme*. Hiebei werden ohne Unterbrechung wechselweise aus den beiden Sendespeichern Blöcke ausgesendet. Die Quittung für den i-ten Block muss während der Sendung des $(i + 1)$-ten Blockes eintreffen. Daraus ergibt sich eine Mindestblocklänge, die durch die Schleifenlaufzeit von Hauptkanal und Rückkanal bestimmt wird. Im CCITT ist ein derartiges System zur Normung vorgeschlagen, das mit

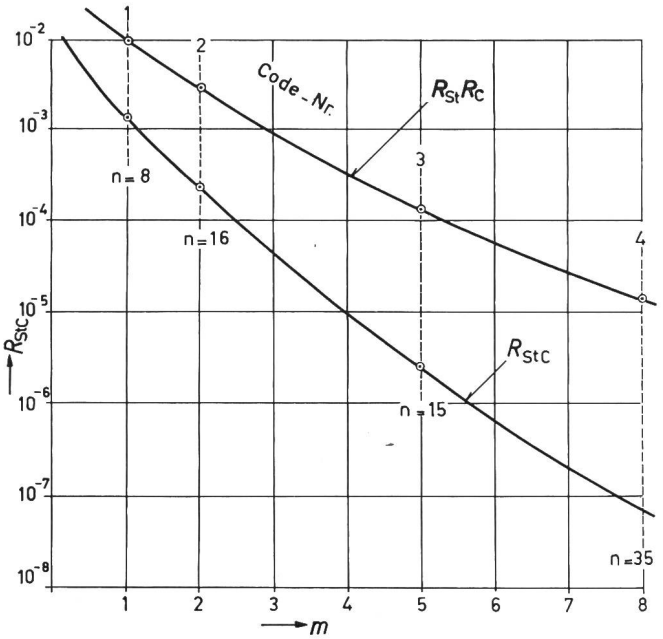


Fig. 9
Fehler-Reduktionsfaktor von Störungsdetektor + Code
Reduktionsfaktor R_{StC} der Blockfehlerwahrscheinlichkeit einer Kombination aus Stördetektor + Code bei Störung von Fernsprechkanälen als Funktion der Anzahl m von Prüfzeichen pro Block. $R_{\text{St}}\, R_{\text{C}}$ = Produkt der Einzelreduktionsfaktoren; Stördetektor = Amplitudentoleranzdetektor; Binärfehlerhäufigkeit: $P_{\text{S}} \approx 10^{-3}$
n = Zahl der Binärzeichen pro Codewort
Generatorpolynome:
Code 1: $g(x) = 1+x$; Code 2: $g(x) = 1+x+x^2$
Code 3: $g(x) = 1+x+x^4+x^5$; Code 4: $g(x) = 1+x+x^3+x^5+x^6+x^8$

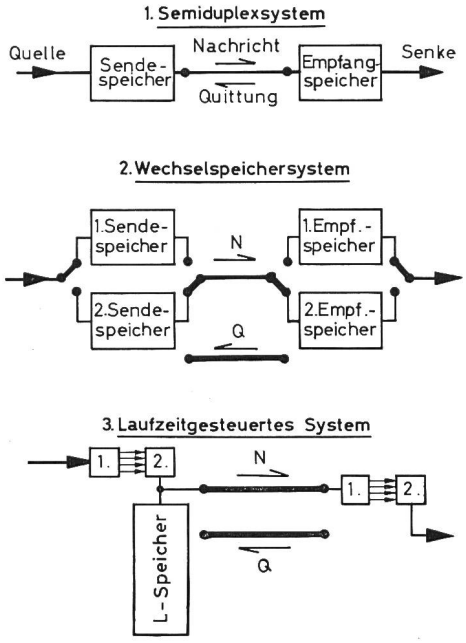


Fig. 10
Prinzipielle Systemorganisationen

Blocklängen von 260, 520 oder 980 bit/Block arbeiten soll. Besonders bei stark gestörten Kanälen liegen die optimalen Blocklängen aber bei wesentlich kleineren Wörtern. Mit lückenloser Übertragung aber von der Schleifenlaufzeit unabhängigen Blocklängen arbeiten die laufzeitgesteuerten Systeme. Die relativ kurzen Blöcke werden gleichzeitig auf den Kanal und in einen sog. L-Speicher gesendet. Der Sender bestimmt die Zeit, die von Aussendung des ersten Blockes bis zum Eintreffen der ersten Quittung vergeht. Mit Hilfe dieser Laufzeitmessung kann er dann genau den Block im L-Speicher bestimmen, für den eine Falschquittung eintrifft. Dieser Block und die während einer Schleifenlaufzeit danach gesendeten Blöcke werden dann wiederholt. Ausführliche Beschreibungen dieser drei Systemtypen findet man in [21; 3; 18].

Ein eingehender Vergleich dieser Systeme wurde anlässlich einer Tagung der NTG über «Teilnehmer Rechensysteme» (September 1968) durchgeführt. Dabei ergab sich, dass laufzeitgesteuerte Systeme bei gleichen Übertragungseigenschaften den kleinsten Speicheraufwand erfordern. Bei Binärfehlerhäufigkeiten $p_s > 10^{-3}$ sind auch bezüglich der effektiven Übertragungsrate diese Systeme den beiden anderen Arten vorzuziehen. Bei $p_s < 10^{-3}$ liefern Wechselspeichersysteme eine höhere Übertragungsrate.

Literatur

[1] *C. E. Shannon* and *W. Weaver:* Mathematical theory of communication. Urbana, Universita of Illinois Press, 1949.
[2] *R. W. Hamming:* Error detecting and error correcting codes. Bell. Syst. techn. J. 29(1950), S. 147...160.
[3] *H. Marko:* Systemtechnik der Datenübertragung auf Fernsprechleitungen. Nachrichtentechnische Fachberichte 19(1960), S. 63...69.
[4] *Deutsche Bundespost:* Study of the general switched telephon network with a view to its suitability for data transmission. Special Study Group A-Contribution Nr. 95, Period 1964/1968.
[5] *Deutsche Bundespost:* Anlage 12 zum Beitrag der Bundesrepublik Deutschland, Sonderkommission A des CCITT. Stellungnahme zu den Punkten A bis O des Studienprogramms. Dokument AP II/8, S. 11...23 und Dokument GT 43 — Nr. 20 der Arbeitsgruppe 43 vom März 1963.
[6] *H. Ohnsorge:* Zusammenhänge zwischen Redundanz und Fehlerwahrscheinlichkeit bei gesicherter Datenübertragung. Dissertation der Rheinisch-Westfälischen Technischen Hochschule Aachen, 1967.
[7] *H. Wolter:* Abschätzung zu Sicherheitssteigerungen einer Nachricht durch automatische Massnahmen ohne Rückfragen. AEÜ 19(1965), S. 317...320.
[8] *W. W. Peterson:* Error-correcting codes. Cambridge (Massachusetts), MIT-Press and New York/London, Wiley, 1961.
[9] *G. Hotz:* Zur mathematischen Theorie der fehlerkorrigierenden Codes. Annales universitatis saraviensis, scientia 9(1960/61)1/2, S. 83...92.
[10] *D. A. Huffmann:* Linear circuit viewpoint on error correcting codes. Trans. IRE Information Theory 2(1956), S. 20...28.
[11] *H. Ohnsorge:* Durch Schieberegister realisierbare reduntate systematische Codes. Telefunken-Ztg. 40(1967), S. 62...69.
[12] *J. M. Wozencraft* and *B. Reiffen:* Sequential decoding. Cambridge (Massachusetts), MIT-Press and New York/London, Wiley, 1961.
[13] *R. G. Gallager:* Low density parity check codes. Cambridge (Massachusetts), MIT-Press, 1963.
[14] *J. L. Massey:* Threshold decoding. Cambridge (Massachusetts), MIT-Press, 1963.
[15] *G. D. Forney:* Concatened codes. Research Monograph Nr. 37. Cambridge (Massachusetts), MIT-Press, 1966.
[16] *J. Ziv:* Asymptotic performance and complexity of a coding scheme for memoryless channels. Trans. IEEE Information Theory 13(1967), S. 356...359.
[17] *H. Marko:* Die Fehlerkorrekturverfahren für die Datenübertragung auf stark gestörten Verbindungen. Nachrichtentechnische Fachberichte 25(1962), S. 101...108.
[18] *U. Haller* und *H. Ohnsorge:* Laufzeitgesteuertes Datenübertragungssystem. Telefunken-Ztg. 40(1967)1/2, S. 76...85.
[19] *F. J. Bloom* et al.: Improvement of binary transmission by null-zone reception. Proc. IRE 45(1957), S. 963...975.
[20] *H. Ohnsorge* und *W. Wagner:* Zur Kombination von Störungsdetektoren und redundanten Codes für die Fehlererkennung. AEÜ 21(1967), S. 487...492.
[21] *F. Schreiber, E. Lukas* und *P. Bocker:* An error correcting data transmission system with block-by-block synchronous operation over telephon channels. IEEE International Convention Record 12(1964)5, S. 73...82.

Adresse des Autors:
Dr. *Horst Ohnsorge,* Allgemeine Elektricitäts-Gesellschaft, AEG-Telefunken, Forschungsinstitut, Elisabethenstrasse 3, D–79 Ulm/Donau.

Commission Internationale de Réglementation en vue de l'Approbation de l'Equipement Electrique (CEE)

Tagung vom 1. bis 12. Oktober 1968 in Oslo

Die diesjährige Herbsttagung der CEE fand auf Einladung des Norwegischen Nationalkomitees in Oslo statt. Von den 19 Mitgliedsländern waren 18 mit 180 Delegierten vertreten. Als Beobachter waren Vertreter aus Kanada, Japan und den USA anwesend. Die Schweiz entsandte 9 Delegierte und war in allen Komitees vertreten. Es fanden Sitzungen der Technischen Komitees für Leitungsschutzschalter, Temperaturregler, Allgemeine Anforderungen, Tragbare Werkzeuge und Motorapparate statt. Den Abschluss bildete die Plenarversammlung und am 12. Oktober die Sitzung des Zulassungsbüros. Anschliessend an den ersten Arbeitstag fand ein Empfang der Delegierten durch den Bürgermeister von Oslo statt.

Komitee für allgemeine Anforderungen (CT 031)

Dem CT 031 unter dem Vorsitz von R. Coutris, Frankreich, standen vom 4. bis 7. Oktober 1968 zwei volle Arbeitstage zur Verfügung. Im Laufe der Besprechung von Verfahrensfragen betreffend die Herausgabe von CEE-Empfehlungen wurde angeregt, dass vor der Einführung neuer Empfehlungen diese den einzelnen technischen Komitees vorgelegt werden und die Komitees dazu Stellung nehmen können. Von entscheidender Bedeutung ist auch, dass möglichst viele Länder mit vorgeschlagenen neuen Prüfverfahren Erfahrungen sammeln.

Anschliessend wurde über die Tätigkeit der verschiedenen Arbeitsgruppen gesprochen. Die Arbeitsgruppe «Hitze und Feuer»