

**Zeitschrift:** Bulletin des Schweizerischen Elektrotechnischen Vereins  
**Herausgeber:** Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätswerke  
**Band:** 64 (1973)  
**Heft:** 8

**Artikel:** Die Anwendung von Galoiskörpern in der Codierungstheorie  
**Autor:** Ohnsorge, H.  
**DOI:** <https://doi.org/10.5169/seals-915540>

### **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:** 03.04.2026

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

# Die Anwendung von Galoiskörpern in der Codierungstheorie <sup>1)</sup>

Von H. Ohnsorge

681.3.053

## 1. Einleitung

Die vorliegende Arbeit soll eine Nutzenanwendung für die Theorie algebraischer Strukturen beschreiben und zeigen, in welcher Weise moderne Algebra praktische Anwendung bei gesicherter Datenübertragung findet.

Die Grundkenntnisse über Mengen, Gruppen, Körper und Vektorräume sowie die Matrizenrechnung werden vorausgesetzt. Zur Vorbereitung werden die Bücher von Kochendörfer, Van der Waerden und Peterson [1; 2; 3]<sup>2)</sup>, empfohlen. Sätze aus der Algebra, die zur Erklärung der redundanten Codierung notwendig sind, werden ohne Beweis gegeben; alle Beweise können den zitierten Büchern entnommen werden. Dieser Aufsatz ist als Querschnitt aus der Theorie der Codierung zu betrachten.

## 2. Begriffe und Definitionen

Eine Code ist die eineindeutige<sup>3)</sup> Abbildung der Elemente einer Menge  $A$  in die Bildmenge  $C$  mit Hilfe der Zuordnung oder Funktion  $\varphi$ , die man als Codiervorschrift bezeichnet.

$a \in A$  wird Buchstabe des Quellenalphabets,  
 $c \in C$  wird Codewort genannt.

Ist  $C \subset M$ , dann handelt es sich um eine redundante Codierung. Entsteht durch eine Störung aus einem Codewort  $c \in C$  ein Element  $m \in M$ , das nicht zur Untermenge  $C$  gehört, dann liegt ein erkennbarer Fehler vor. Wird durch eine Funktion  $\psi_3$  jedes Element  $m \in M$  in die Untermenge  $C$  eindeutig abgebildet, dann ist  $\psi_3$  die Fehlerkorrekturvorschrift (häufig auch Decodiervorschrift genannt, obgleich das leicht zur Verwechslung mit der Umkehrfunktion bzw. der inversen Abbildung von  $\varphi(a)$  führt, die ebenfalls Decodiervorschrift heisst). Entsteht durch die Störung des Elementes  $c_1$  ein Element  $c_j$ , das auch der Menge  $C$  angehört, dann kann mit Hilfe des Codes dieser Fehler nicht erkannt werden, denn einem Codewort lässt sich natürlich nicht ansehen, dass es durch Störungen aus einem anderen entstanden ist. Nicht erkennbare Fehler lassen sich selbstverständlich auch nicht korrigieren. Entsteht durch eine Störung aus dem Element  $c_1 \in C$  ein falsches Element  $m = F(c_1) \in M$ , das nicht zu  $C$  gehört und bei der Decodierung  $c_j = \psi_3(m) \neq c_1$ , dann liegt in diesem Fall eine fehlerhafte Korrektur vor: Der aufgetretene Fehler ist erkennbar aber nicht korrigierbar. Mit anderen Worten:

Die Decodiervorschrift  $\psi_3$  bildet Teilmengen  $T$  von  $M$  in ein einziges Element aus  $C$  ab und ist daher nicht umkehrbar eindeutig. Entsteht bei der Störung aus  $c_1$  ein Element der Teilmenge  $T_j$ , die durch  $\psi_3$  in  $c_j$  abgebildet wird, dann haben die

Störungen ein nichtkorrigierbares Fehlermuster erzeugt. Ein optimaler fehlerkorrigierender Code liegt dann vor, wenn  $\psi_3$  so gewählt wird, dass die Wahrscheinlichkeit für nicht korrigierbare Fehler minimal wird. Daraus folgt sofort, dass  $\psi_3$  nicht unabhängig von der zu erwartenden Stör- oder Fehlerstruktur optimal gewählt werden kann.

Die vorangegangenen Definitionen oder Begriffe seien im folgenden an einem Beispiel erklärt.

Das Quellenalphabet  $A$  bestehe aus der Menge der Dezimalziffern und den Symbolen für die elementaren Verknüpfungen also

$$A = (0; 1; 2; 3; 4; 5; 6; 7; 8; 9; +; -; \times; :; ,; =)$$

Die  $q = 16$  Alphabetbuchstaben können durch  $k$ -Tupel aus Binärzahlen 0 und 1 dargestellt werden, wenn  $k = ldq = 4$  gewählt wird, z.B.

0	→	0 0 0 0	
1	→	0 0 0 1	
2	→	0 0 1 0	
3	→	0 0 1 1	
.		.	Zuordnung oder Codiertabelle (Codebuch)
.		.	
.		.	
,	→	1 1 1 0	
=	→	1 1 1 1	
<u>A</u>		<u>C<sub>1</sub></u>	(1)

Dieser nichtredundante Code benutzt als Codiervorschrift  $\varphi_1$  einfach eine Zuordnungstabelle.

Weitere in der Codierungstheorie definierte Begriffe werden im folgenden Text kursiv gesetzt und es empfiehlt sich – soweit keine Erklärungen im Text dafür gegeben sind – die Definitionen z.B. aus [3] zu entnehmen.

## 3. Matrixdarstellung der redundanten Codes

### 3.1 Darstellung der Codes durch die Basismatrix

Die von 0 verschiedenen  $k$ -Tupel eines nichtredundanten Codes lassen sich als *Linearkombinationen* der *Zeilenvektoren* einer *Einheitsmatrix*  $[I_1]$  darstellen:

$$\begin{matrix} 1. & \left[ 1 & 0 & 0 & 0 \right] \\ 2. & \left[ 0 & 1 & 0 & 0 \right] \\ 3. & \left[ 0 & 0 & 1 & 0 \right] \\ 4. & \left[ 0 & 0 & 0 & 1 \right] \end{matrix} = [I_1] = [G] \quad (2)$$

Die Komponenten dieser Matrix sind Elemente des *Galois-Feldes*  $GF(2)$ , die *Addition* entspricht dabei der *modulo 2-Arithmetik*. Die Menge der *linear unabhängigen Vektoren* deren Gesamtheit von *Linearkombinationen* die Menge  $C_1$  mit Ausnahme des Nullvektors liefert, nennt man *Basis*  $G$  des Code.

<sup>1)</sup> Vortrag, gehalten am 10. Februar 1972 an der Universität Bern.

<sup>2)</sup> Siehe Literatur am Schluss des Aufsatzes.

<sup>3)</sup> In dieser Arbeit werden nur eineindeutige Codes betrachtet. Stellt man z. B. Analogsignale durch Digitalsignale dar, dann liegt eine nicht umkehrbar eindeutige Codierung vor.

Den Nullvektor [0 0 0 0] könnte man als Kombination 0-ter Klasse auffassen.

Wählt man als Codewörter eines Codes  $C_2$   $n$ -Tupel mit z.B.  $n = 7$ , dann besteht die Menge  $M$  aller binären 7-Tupel aus  $2^7 = 128$  Elementen. Da aber  $A$  und damit  $C_1$  und  $C_2$  nur  $2^k = 2^4 = 16$  Elemente enthält, sind in  $M$   $128 - 16 = 112$  Elemente, die nicht zum Code gehören. Das heißt jedes Codewort enthält 3 überflüssige bzw. *redundante Binärzeichen* oder *Prüfzeichen*. Die Basis dieses redundanten Codes  $C_2$  muss zunächst einmal wieder die Einheitsmatrix enthalten, da dann die  $k = 4$  für die Information (Elemente aus  $A$ ) erforderlichen Positionen, wie bei dem nichtredundanten Code gebildet werden können. Die Besetzung der  $n - k = m$  Positionen für die Prüfzeichen geschieht mit Hilfe der *Codiervorschrift*  $\varphi_2$  ( $C_1$ ) und ist eine Problemstellung der Codierungstheorie. Wählt man in unserem Beispiel als Basis die Matrix

$$\begin{aligned} 1. &= \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [G] = [I_1, P] \\ 2. & \\ 3. & \\ (k = 4.) & \end{aligned} \quad (3)$$

dann bildet  $C_2$  eine *additive Abelsche Gruppe* mit dem 0-Vektor [0 0 0 0 0 0 0] als *Identitäts- oder Einselement*, wie in Abschn. 3.2 gezeigt wird. Derartige Codes heißen *Gruppen-Codes*.  $[G]$  besteht also aus der Basis  $[I_1]$  des nichtredundanten Codes ergänzt um eine geeignet ausgewählte Matrix  $[P]$ , die Redundanz- oder Prüfzeichenmatrix genannt sei. Die Zeilen von  $[G]$  sind wegen  $[I_1]$  linear unabhängig, daher existieren, wie gefordert,  $2^k = 2^4 = 16$  Elemente bzw. Vektoren in  $C_2$ , denn die Summe der Kombinationen über alle Klassen von  $k$  Elementen beträgt

$$\sum_{i=0}^k \binom{k}{i} = 2^k$$

Zu den Vektoren aus  $C_2$  existiert eine Menge  $O$  von Vektoren, die orthogonal zu den Elementen aus  $C_2$  sind: d.h. das *innere oder Skalarprodukt* beliebiger Elemente  $c_{2i} \in C_2$  und  $0_j \in O$  ist gleich null, also  $c_{2i} \cdot 0_j = 0$ .

In unserem Beispiel hat  $O$  eine Basis der Form

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} = [B] \quad (4)$$

Zur Vervollständigung der Begriffe, die im Weiteren benutzt werden, sei noch ohne Erläuterung folgendes bemerkt:

In unserem Beispiel ist  $C_2$  mit der Basis  $[G]$  ein  $k$ -dimensionaler Vektorraum über dem Körper bzw. dem Galoisfeld  $GF(2)$  und die Menge  $O$  ist der zugehörige *Orthogonalraum* mit der Dimension  $n - k = m$ .  $C_2$  und  $O$  sind *Unterräume* der Menge  $M$  bzw. des Raumes aller  $n$ -Tupel mit binären Komponenten.

Die Zahl der Komponenten, um die sich zwei Vektoren oder Codewörter  $c_{2i}$ ,  $c_{2j}$  unterscheiden, nennt man *Hammingdistanz*  $d^+$  also

$$\begin{aligned} \text{z.B. } c_{21} &= 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 & \text{[siehe Gl. (3)]} \\ c_{24} &= 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \\ d^+ &= 1 + 1 + 1 + 1 = 4 \end{aligned} \quad (5)$$

Eine Störung kann nur dann ein Codewort in ein anderes Codewort verfälschen, wenn von der Störung  $d^+$  Binärfehler erzeugt werden. Die kleinste Hammingdistanz, die in einem Code  $C$  auftritt, wird *Minimumdistanz*  $d$  genannt. Es ist nach dem vorhergehenden Satz leicht einzusehen, dass ein Code mit der Minimumdistanz  $d$  in der Lage ist, alle Kombinationen mit  $i < d - 1$  Binärfehlern in einem Codewort zu erkennen. Die Zahl der «1»-en in einem binären Codewort nennt man das *Gewicht*  $W$  des Codewortes.

Haben die  $n$ -Tupel der Teilmenge  $T_i$ , die durch die Decodiervorschrift  $\varphi_3$  in ein Codewort  $c_{2i}$  abgebildet werden, die kleinstmögliche Distanz von  $c_{2i}$ , und besitzen alle Codewörter in  $C_2$  Teilmengen  $T$  mit gleichviel Elementen, dann liegt ein *dichtgepackter Code* vor. Diese Codes sind optimal für statistisch unabhängig auftretende Binärfehler. In unserem Beispiel ist  $C_2$  ein derartiger Code (Hamming-Code). Der Raum aller  $n$ -Tupel ist, durch die Codewörter eines dichtgepackten Codes homogen ausgefüllt, d.h. die *Distanzverteilung* der Codewörter gegenüber einem Codewort  $c_{2i}$  ist für jedes Codewort gleich. Diese Eigenschaft haben alle *Gruppencodes*, was aber nicht heißt, dass alle Gruppencodes dichtgepackte Codes sind. Im Gegenteil: es existieren kaum dichtgepackte Codes (bekannt sind z.B. Hamming-Codes und der Golay-Code). Existiert für gegebenes  $n$  und  $k$  [ $(n, k)$ -Codes] kein dichtgepackter Code, dann ist der Code optimal für statistisch unabhängige Fehler, welcher der «dichten Packung» am nächsten kommt (z.B. *quasidichtgepackte Codes*).

Der Vektorraum  $V$  aus  $n$ -Tupeln mit Komponenten aus  $GF(2)$  besitzt  $2^n$  Elemente. Für den Code  $C_2$  werden aber davon nur  $2^k$  Elemente benötigt, also bleiben bei gleichmässiger Verteilung pro Codewort Teilmengen  $T$  mit  $(2^n/2^k) - 1 = 2^m - 1$  nicht benötigten Elementen. Im Abstand  $d^+ = 1$  von  $c_{2i}$  liegen in  $V$  insgesamt  $\binom{n}{1} = n$  Elemente, im Abstand  $d^+ = i$  liegen  $\binom{n}{i}$  Elemente. Wählt man also  $T$  so aus, dass ein dichtgepackter Code entsteht, dann ist

$$2^m - 1 = \sum_{i=1}^e \binom{n}{i} \quad (5.1)$$

Falls diese Gleichung nicht existiert, d.h. dass bei gegebenem  $(n, e)$ ,  $(n, m)$  oder  $(m, e)$  kein dichtgepackter Code konstruiert werden kann, dann muss

$$2^m - 1 > \sum_{i=1}^e \binom{n}{i} \quad (5.2)$$

gewählt werden.

Aus Gl. (5.1) und (5.2) folgt die sogenannte *Hamminggrenze*

$$m \geq \text{ld} \sum_{i=0}^e \binom{n}{i} \quad (5.3)$$

die aussagt, dass ein Code der Codewort- oder *Blocklänge*  $n$  mindestens  $\text{ld} \sum_{i=0}^e \binom{n}{i}$  Prüfzeichen besitzen muss, wenn alle Muster mit  $i = 1$  bis  $e$  Binärfehlern korrigierbar sein sollen. Wählt man  $m$  Prüfzeichen, dann hat der zugehörige nichtredundante Code  $C_1$   $k = n - m$  Informationsstellen. Beim  $e$  Fehler korrigierenden Code beträgt die Minimumdistanz  $d = 2e + 1$ , bzw. ist  $e = \frac{d-1}{2}$ .

### 3.2 Darstellung linearer systematischer Codes durch die Codier- und Decodiermatrix

Unterscheiden wir  $q$  Elemente, wobei  $q$  eine Primzahlpotenz ist, dann bilden diese Elemente einen *endlichen Körper*  $F$ . Die Menge aller  $n$ -Tupel aus diesen Körperelementen bilden einen Vektorraum, die Elemente eines *Unterraumes* im Rahmen aller  $n$ -Tupel über  $F$  bilden einen linearen Code. Über jedem Körper aus  $p$  Elementen, bei dem  $p$  eine Primzahl ist, bildet eine Menge von Vektoren, die eine Gruppe darstellen, einen linearen Raum. *Binäre Linearcodes* werden daher auch *Gruppencodes* genannt. Bildet man aus einem nichtredundanten Code  $C_1$  einen redundanten Code  $C_2$ , der nur durch Anhängen von Prüfzeichen an die Codewörter  $C_1$  (an die *Informationsstellen*) entsteht, dann heisst dieser Code *systematisch*. Werden durch *lineare Verknüpfung* von Informationselementen die einem Körper  $F$  angehören, Prüfzeichen abgeleitet und im Anschluss an die unveränderten Informationsstellen gesendet (= Codiervorschrift  $\varphi_2$ ), dann liegt ein *linearer systematischer Code* vor.

Die Informationsstellen, also die Komponenten der Codewörter von  $C_1$ , seien  $x_1 x_2 \dots x_k$  aus  $GF(2)$ . Zur linearen Verknüpfung benutzt man die Matrix  $[A]$  mit Koeffizienten aus  $GF(2)$ , so dass der *Prüfzeichenvektor* oder die *Prüfzeichenmatrix*  $[y_1 y_2 \dots y_m]$  sich aus

$$[A] \cdot [X]_I^T = [Y]^T \quad (6)$$

ergibt.

wobei  $[X]_I = [x_1, x_2, \dots, x_k]$  die *Informationszeichenmatrix* und  $[X]_I^T$  die transponierte Matrix  $[X]_I$  ist. Nennen wir  $y_i = x_{k+i}$ , dann wird aus Gl. (6) ein homogenes Gleichungssystem, bei dem  $[A]$  durch die Einheitsmatrix  $I_2$  ergänzt ist und  $[X]$  die Codewörter bilden, also:

$$\begin{aligned} [A, I_2] \cdot [X]^T &= [O] = [B] \cdot [X]^T \\ [X] &= [x_1 x_2 \dots x_k x_{k+1} = y_1 x_{k+2} = y_2 \dots x_{k+m} = y_m] \quad (7) \\ [X] &\in C_2 \end{aligned}$$

$[A]$  wird *Codier-* und  $[B]$  *Decodiermatrix* genannt. Die Linearkombinationen von  $[B]$  bilden den Orthogonalraum zum Code  $C_2$ . Wir benutzen wieder unser Beispiel und entnehmen aus Gl. (4)

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} = [A] \quad \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} = [B] \quad (8)$$

und wir erhalten

$$\begin{aligned} [A] \cdot [I_1]^T &= [P]^T \text{ mit } [I]^T = [I] \\ \text{bzw.} \quad [A, I_2] \cdot [I_1, P]^T &= [O] = [B] \cdot [G]^T \quad (9) \end{aligned}$$

In Worten: Die Codiermatrix  $[A]$  multipliziert mit der Einheitsmatrix  $[I_1]$ , die immer die Basismatrix der Informationsstellen bzw. des nichtredundanten Codes  $C_1$  ist, liefert die transponierte *Redundanzmatrix*  $[P]$  der *Basis*  $[G]$  des Codes  $C_2$ .  $[A]$  um  $[I_2]$  ergänzt liefert  $[B]$ ;  $[I_1]$  um  $[P]$  ergänzt liefert  $[G]$ ; und  $[G]$  ist orthogonal zu  $[B]$ .

Durch Störungen wird das Codewort  $[X]$  in ein Empfangswort  $[X_e]$  verfälscht, dies kann man sich durch Addition eines Fehlerwortes  $[X_f]$  zu  $[X]$  vorstellen, also

$$\begin{aligned} [X_e] &= [X] + [X_f] \\ \text{z. B. } c_{21} &= [X] = 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \\ [X_f] &= 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \\ [X_e] &= 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \\ &\quad \uparrow \quad \uparrow \quad \uparrow \\ &\quad \text{Fehler} \end{aligned} \quad (10)$$

Zur Decodierung wird zunächst

$$[B] \cdot [X]_e^T = \underbrace{[B] \cdot [X]^T}_0 + [B] \cdot [X_f]^T = [S] \quad (11)$$

gebildet.

$[S]$  das sog. *Syndrom* ist eine einspaltige Matrix mit  $m$  Komponenten aus  $GF(2)$  und hängt nur von dem Fehlerwort  $[X_f]$  ab, da per Definition bzw. Codiervorschrift jedes Codewort orthogonal zu  $[B]$  ist.  $[B] \cdot [X]^T \rightarrow [S]$  ist eine eindeutige aber nicht umkehrbar eindeutige Abbildung von  $[X_f]$  in  $[S]$ , da  $[X_f]$   $2^n - 1$  von  $[O]$  verschiedene Elemente besitzt,  $[S]$  dagegen nur  $2^m - 1$  von  $[O]$  verschiedene Elemente hat. Erhalten wir  $[B] \cdot [X_f]^T = [O] = [S]$  dann ist  $[X_f]$  entweder  $[O]$  oder ein Codewort  $[X]$ , im letzteren Fall liegt also ein nicht erkennbares Fehlermuster vor. Bei  $[S] \neq [O]$  ist ein Fehlermuster erkannt. Fordert man, dass der Code eine Menge  $F^+$  von Fehlermustern korrigieren können soll; dann muss  $F^+$  durch  $[B]$  eineindeutig in die Menge  $[S]$  abgebildet werden. Ist  $f \in F^+$ ;  $t_i \in T_i$  und gehört  $T_i$  zu  $c_{2i}$ , dann gilt  $t_i = c_{2i} + f$  für alle Elemente aus  $T_i$ . Sollen z. B. alle Fehlermuster mit  $1 \leq i \leq e$  Binärfehlern korrigierbar sein, dann muss die Zahl der von  $[O]$  verschiedenen

Synndrome  $Z = 2^m - 1$  mindestens gleich  $\sum_{i=1}^e \binom{n}{i}$  d. h. gleich der Summe von Kombinationen  $i$ -ter Klasse von  $n$  Elementen sein; ist  $Z > \sum_{i=1}^e \binom{n}{i}$ , dann sind auch noch einige Muster mit mehr als  $e$  Fehlern korrigierbar. Aus dieser Betrachtung folgt ebenfalls die Hamminggrenze:

$$\begin{aligned} 2^m - 1 &\geq \sum_{i=1}^e \binom{n}{i} \\ m &\geq \text{ld} \sum_{i=0}^e \binom{n}{i} \end{aligned} \quad (12)$$

Mit  $[B]$  lässt sich nun zu jedem Fehlermuster  $[X_f]_i$  das korrigierbar sein soll, das zugehörige Syndrom  $[S]_i$  berechnen. Tritt beim Decodierprozess ein  $[S]_i \neq [O]$  auf, dann wird das zugehörige Fehlermuster  $[X_f]_i$  vom Empfangswort subtrahiert und man erhält das korrigierte Codewort

$$[X] = [X_e] - [X_f]_i \quad (13)$$

solange  $[X_f]_i = f_i \in F^+$ , andernfalls erfolgt fehlerhafte Korrektur (= erkennbarer aber nicht korrigierbarer Fehler).

Als nächstes wenden wir uns der Frage zu, wie muss  $[A]$  gewählt werden, damit ein optimaler (dichtgepackter oder möglichst dichtgepackter) Code gegen statistisch unabhängige Fehler entsteht.

Zur Vereinfachung schreiben wir  $[B] \cdot [X_f]^T = [S]$  in die anschauliche Form:

$$\begin{bmatrix} x_{f1} & x_{f2} & \dots & x_{fn} \\ b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & & & \cdot \\ \cdot & & & \cdot \\ b_{m1} & \dots & \dots & b_{mn} \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \dots \\ s_m \end{bmatrix} \quad (14)$$

$[b]_1 \qquad \qquad \qquad [b]_m$

Z.B. sei entsprechend Gl. (10) und (8):

$$\begin{aligned}
 [X_f] &\rightarrow [0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0] \\
 &\quad \downarrow \quad \downarrow \quad \downarrow \\
 [B] &\rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \end{bmatrix} = [S] \quad (15)
 \end{aligned}$$

Man erkennt also, dass das Syndrom gleich der Summe der Spaltenvektoren  $[b]_i$  ist, die zu einer «1» im Fehlerwort bzw. zu einem Fehler im Codewort gehören:

$$[S] = \sum_{x_i=1} [b]_i \quad (16)$$

Ist die Zahl  $e$  der korrigierbaren Einzelfehler in den Codewörtern der Länge  $n$  vorgegeben, dann ergibt sich aus Gl. (5,1) die Mindestkomponentenzahl  $m$ . Aus der Menge aller  $m$ -Tupel über  $GF(2)$  müssen die Spalten von  $[B]$  nun so ausgewählt werden, dass mindestens  $d-1 = 2e$  beliebige Spaltenvektoren von  $[B]$  linearunabhängig sind, denn erst bei  $d$  Fehlern im Codewort darf  $[S] = [O]$  – also ein nicht erkennbarer Fehler – entstehen, d.h. erst eine Linearkombination aus  $d-1$  Spalten  $[b]_i$  darf eine weitere Spalte entstehen lassen, die bei  $d$  Fehlern im Codewort zu  $[S] = [O]$  führen kann. Gelingt diese

Spaltenauswahl bei  $m = \text{ld} \sum_{i=0}^e \binom{n}{i}$ , dann ist ein dichtge-

packter Code gefunden, andernfalls muss man  $m$  um 1, 2... $i$  vergrößern bis  $[B]$  die Forderung bezüglich der linearen Unabhängigkeit seiner Spalten erfüllt.  $m$  Spalten sind durch die Einheitsmatrix vorweggenommen. Ausserdem bilden  $d-1$  Spalten der Einheitsmatrix als Linearkombination immer eine Spalte mit  $d-1$  «1»-en; die Spalten der Matrix  $[A]$  müssen also mindestens  $d-1$  «1»-en aufweisen. Mehr Anhaltspunkte für die Konstruktion der Codier- und Decodiermatrix zur Erzeugung möglichst dichtgepackter Codes existieren nicht, so dass  $[B]$  nur mit Hilfe eines Computers durch das «trial and error»-Verfahren bestimmt werden kann.

Wesentlich weiter kommt man bei dem Problem der Codekonstruktion durch die Polynomdarstellung linearer Codes.

#### 4. Polynomdarstellung der linearen Codes

Die Menge aller  $n$ -Tupel mit den Komponenten  $x_i$  aus einem Körper  $F$  z.B. aus  $GF(p)$  können als Koeffizientenmatrix von Polynomen der Form

$$f(X) = x_0 + x_1X + x_2X^2 + \dots + x_{n-1}X^{n-1} \quad (17)$$

aufgefasst werden mit  $X$  als Operator (auch *Verschiebeoperator* genannt).

Es ist also

$$f(X) \in M = \text{Menge aller Polynome vom Grad } < n \text{ über } F \quad (18)$$

$M$  entsteht aus der Menge aller Polynome  $F(X)$  über  $F$  modulo einem Polynom  $f^*(X)$  mit Koeffizienten aus  $F$  als Repräsentanten der Restklassen  $\{f(X)\}$ ; d.h.  $f(X)$  ist jeweils das Polynom vom kleinsten Grade in der Restklasse  $\{f(X)\}$ .

Man erhält  $f(X)$  aus  $F(X)$  durch den *Euklidischen Divisionsalgorithmus*.

$$\frac{F(X)}{f^*(X)} = q(X) + \frac{f(X)}{f^*(X)} \quad (19)$$

Die Menge der Restklassen  $\{f(X)\}$  bildet eine *kommutative, lineare assoziative Algebra*  $A$  und erfüllt damit alle Axiome der *algebraischen Strukturen*: Gruppe, Ring und Vektorraum. Wählt man ausserdem für  $f^*(X)$  ein über  $F$  *irreduzibles Polynom*  $p(X)$  vom Grade  $K$ , dann ist die Algebra der Polynome über  $F$  modulo  $p(X)$  auch ein Körper und zwar *der Erweiterungskörper vom Grade  $K$  über dem Grundkörper  $F$*  bzw. ein *Galoisfeld*  $GF(p^K)$ , wenn  $F = GF(p)$ , also ein Primzahlkörper ist.

Ein *Ideal*  $I$  ist definiert als Untermenge von Elementen eines Ringes  $R$ , die Untergruppe der additiven Gruppe von  $R$  ist und für die gilt:  $a \in I; r \in R \Rightarrow ar$  und  $ra \in I$ . Besteht das Ideal aus allen Vielfachen eines Ringelementes  $r$ , dann heisst es *Hauptideal*. Eine Menge von Polynomen bildet dann und nur dann ein Ideal, wenn sie aus allen Vielfachen eines Polynoms  $g(X)$  besteht.

Wählen wir

$$f_i(X) = q_i(X) \cdot g(X) \in C_2 \subset M \quad (20)$$

wobei  $q_i(X)$  ein beliebiges Polynom vom Grade  $\leq k-1 = n-m-1$  und  $g(X)$  ein *normiertes Polynom* vom Grade  $m$  ist – mit Koeffizienten aus  $F$  bei allen Polynomen – dann bildet die Menge  $C_2$  der Polynome  $f_i(X)$  ein *Hauptideal*  $I$  in der Algebra  $A$ , das von  $g(X)$  erzeugt wird, wenn  $g(X)$  Teiler von  $f^*(X)$  ist.

(Mit Hilfe des *Nebenklassenschemas* kann man durch dieses Ideal  $I$  einen Restklassenring bilden, dieser heisst *Polynomring modulo  $f^*(X)$* .  $I$  bildet den Code  $C_2$  bzw. die Restklasse  $\{O\}$ ; die Repräsentanten  $f(X)$  der weiteren Restklassen  $\{f(X)\}$  sind Elemente der Mengen  $T$ , in denen die für den Code  $C_2$  nicht verwendeten  $n$ -Tupel liegen).

$I$  stellt in  $A$  einen *Unterraum* dar mit den Basisvektoren

$$\{g(X)\} \{X \cdot g(X)\} \dots \{X^{k-1} \cdot g(X)\} \quad (21)$$

da nach Gl. (20) jedes Codewort als Linear-Kombination dieser Vektoren gebildet werden kann, denn es ist

$$c_{2i} = f_i(X) = (q_0 + q_1X + q_2X^2 \dots q_{k-1}X^{k-1}) \cdot g(X) \quad (22)$$

mit  $g(X) = g_0 + g_1X + g_2X^2 \dots g_mX^m$

Als Beispiel wählen wir

$$\begin{aligned}
 f^*(X) &= 1 + X^7 \\
 g(X) &= 1 + 0 + X^2 + X^3 \\
 \{g(X)\} &= \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [G] \quad (23) \\
 \{X \cdot g(X)\} &= \\
 \{X^2 \cdot g(X)\} &= \\
 \{X^3 \cdot g(X)\} &=
 \end{aligned}$$

Gemäss obiger Forderung für  $I$  wurde  $g(X)$  als Teiler von  $f^*(X)$  gewählt. In unserem Beispiel ist

$$\frac{f^*(X)}{g(X)} = h(X) + 0 \quad (24)$$

$$\frac{X^7 + 1}{x^3 + x^2 + 1} = 1 + 0 + x^2 + x^3 + x^4 = h(X) \quad (25)$$

In der Algebra  $A$  der Polynome über  $F$  modulo  $f^*(X)$  ist das Ideal, das von  $h(X)$  gebildet wird, orthogonal zu dem von  $g(X)$  gebildeten Ideal, da

$$\begin{aligned} \{a(X)h(X) \cdot q(X)g(X)\} &= \{a(X) \quad q(X)\} \cdot \{h(X)g(X)\} \\ &= \{a(X) \quad q(X)\} \cdot \{0\} = 0 \end{aligned} \quad (26)$$

Polynome gelten als *orthogonal*, wenn deren Produkt in der Algebra  $A$  null ist, also z. B.:

$$g(X)h(X) \text{ modulo } f^*(X) = 0 \quad (27)$$

Bildet man das Produkt der Koeffizientenmatrizen  $[g] \cdot [h]^T$ , dann ist dieses nur dann 0, wenn man eine *Umkehrung der Indizes* von  $h$  oder  $g$  vornimmt, also

$$[g_0, g_1, g_2, \dots, g_m] \cdot \begin{bmatrix} h_k \\ h_{k-1} \\ \vdots \\ h_0 \end{bmatrix} = 0 \quad (28)$$

bei  $f^*(X) = X^n + 1$ .

Die Basis  $H^*$  des von  $h(X)$  gebildeten Ideals hat folgende Form bei

$$\begin{aligned} f^*(X) &= 1 + x^7 \\ h(X) &= 1 + 0 + x^2 + x^3 + x^4 \\ \{h(X)\} &= \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \\ \{X \cdot h(X)\} &= \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \\ \{X^2 \cdot h(X)\} &= \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \end{aligned} = [H]^* \quad (29)$$

Vertauschen wir die Komponenten von Gl. (29) zu

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} = [H] \quad (30)$$

dann gilt mit  $[G]$  nach Gl. (23):

$$\begin{aligned} [G] \cdot [H]^T &= 0 \\ [H] \cdot [G]^T &= 0 \end{aligned} \quad (31)$$

Gl. (31) bleibt gültig, wenn in  $[H]$  und  $[G]$  die gleichen Spaltenvertauschungen vorgenommen werden. Bilden wir aus  $[H]$  nach Gl. (30) die Decodiermatrix  $[B]$  nach Gl. (15), dann erhält  $[G]$  die Form  $[G]^*$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} = [G]^* \quad (32)$$

mit

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} = [H]^* = [B] \text{ und } [B] \cdot [G]^* = 0$$

Durch *elementare Zeilenoperationen* lässt sich aus  $[G]^*$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [G] \text{ nach Gl. (3) bilden} \quad (33)$$

Es gilt natürlich wieder

$$[B] \cdot [G]^T = 0 \quad (34)$$

entsprechend Gl. (9).  $g(X)$  und  $f^*(X)$  beschreiben den Code  $C_2$  genauso vollständig wie  $[A]$  und  $n$  bei der Matrixdarstellung.  $g(X)$  wird *Basis- oder Generatorpolynom* genannt.

Für  $f^*(X) = X^n - 1$  bildet das von  $g(X)$  erzeugte Ideal  $I$  einen *zyklischen Unterraum* in der Algebra  $A$ ; der Code  $C_2$  mit dem Generatorpolynom  $g(X)$  das  $f^*(X) = X^n - 1$  teilt, heisst daher *zyklischer Code*. Jede zyklische Verschiebung der Komponenten eines Codeworts liefert wieder ein zum Code  $C_2$  gehöriges  $n$ -Tupel, z. B.

$$\begin{aligned} [X]_i &= \{X^3 g(X)\} = [0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1] = \text{Codewort } c_1 \\ [X]_{2i} &= \{X^4 g(X)\} = [1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1] = \text{Codewort } c_j \end{aligned} \quad (35)$$

Binärcodes, die von einem Polynom  $g(X)$  erzeugt werden, lassen sich sehr einfach durch rückgekoppelte Schieberegister erzeugen. Die zyklischen Codes dieser Klasse eignen sich besonders zur Korrektur von *Fehlerbündeln (error bursts)*, das sind ganz allgemein kurze Zeitintervalle hoher Störungsintensität bzw. Sequenzen mit hoher Binärfehlerwahrscheinlichkeit. In einem Codewort oder Block ist ein *Burst* definiert als die Folge von Zeichen, gezählt vom ersten bis zum letzten Fehler im Block. Entsprechend Gl. (15) und (16) wird ein Fehlerburst, der allein Prüfstellen umfasst, direkt im Syndrom, gespiegelt an der Einheitsmatrix, abgebildet. Jeder Fehlerburst  $B(X)$  der Länge  $b \leq m$  kann also durch zyklische Vertauschung der Komponenten eines Empfangswortes  $[X_e]$  so verschoben werden, dass ein  $[X_e]_{zi}$  entsteht, dessen letzte  $m$  Positionen den Burst enthalten. Das Produkt

$$\begin{aligned} [B] [X_e]_{zi}^T &= \underbrace{[B] \cdot [X]_{zi}^T}_0 + [B] [X_f]_{zi}^T = [B] \cdot [X_f]_{zi}^T = \\ &= [S] \hat{=} B(X) \end{aligned} \quad (36)$$

liefert dann ein Syndrom, dessen Komponenten die Koeffizienten des Polynoms sind, das den Burst  $B(X)$  beschreibt. Benützt man zur Lokalisierung des Burst z. B. eine Störungsmessung (*Stördetektor*), dann ist es möglich, entsprechend Gl. (13) und (36) Bursts bis zur Länge  $m$  zu korrigieren. Ohne Stördetektor wird mindestens die Hälfte der Redundanz zur *Burstlokalisierung* benötigt, so dass bei günstigen Codes nur Bursts der Länge  $b \leq m/2$  korrigiert werden können. Verfahren zur Fehlerkorrektur können in diesem Rahmen nicht eingehend diskutiert werden, es sei daher auf die zusammenfassende Arbeit [4] hingewiesen, die hinreichende Literaturangaben zum Weiterstudium enthält.

Mit Gl. (20) ist bereits ein Bildungsgesetz für Codewörter eines zyklischen Codes gegeben:

Die Koeffizienten von  $q_i(X)$  können als die Informationszeichen eines Codewortes entsprechend  $[X]_i$  nach Gl. (6) angesehen werden, das Codewort

$$c_i = f_i(X) = q_i(X) \cdot g(X) \quad (37)$$

enthält dann aber die Informationsstellen nicht mehr in unveränderter Folge; der Code ist nicht systematisch.

Mit Hilfe des Euklidischen Divisionsalgorithmus lässt sich aber auch durch  $g(X)$  ein Ideal erzeugen, das einem systematischen Code entspricht: Es sei  $f_i(X)$  ein Polynom der Form

$$f_i(X) = x_{n-1} X^{n-1} + x_{n-2} X^{n-2} \dots + x_m X^m + 0 + 0 \dots + 0 \quad (38)$$

dessen Koeffizienten den Komponenten von  $[X]_{fi}$  entsprechen. Bilden wir

$$\frac{f_i(X)}{g(X)} = q(X) + \frac{r(X)}{g(X)}$$

bzw.

$$f_i(X) - r(X) = q(X) \cdot g(X) = f(X) \quad (39)$$

dann ist  $f(X)$  ein Codewort entsprechend Gl. (20) oder (37), das in den ersten  $k$  Positionen die unveränderten Informationszeichen enthält; die letzten  $m$  Positionen – also die Koeffizienten von  $r(X)$  – bilden die Prüfzeichen. Der euklidische Divisionsalgorithmus kann auch zur Berechnung des Syndroms  $[S] = S(X)$  benutzt werden, indem man

$$\begin{aligned} \frac{f_e(X)}{g(X)} &= \frac{f(X) + f_i(X)}{g(X)} = \frac{q(X)g(X)}{g(X)} + \frac{f_i(X)}{g(X)} = \\ &= q(X) + q_f(x) + \frac{r_f(X)}{g(X)} \quad (40) \end{aligned}$$

bzw.

$$f_e(X) \text{ mod. } g(X) = r_f(X) = S(X)$$

bildet, wobei  $f_i(X)$  das Fehlerwort repräsentiert. Benutzen wir Beispiel Gl. (10) mit

$$\begin{aligned} [X] &= [1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0] = X^6 + 0 + 0 + 0 + X^2 + X + 0 = f(X) \\ [X_f] &= [0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0] = 0 + X^5 + 0 + X^3 + X^2 + 0 + 0 = f_i(X) \\ [X_e] &= [1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0] = X^6 + X^5 + 0 + X^3 + 0 + X + 0 = f_e(X) \end{aligned} \quad (41)$$

dann erhalten wir nach Gl. (15)  $[S] = [0 \ 1 \ 0]$  und mit Gl. (40):

$$\begin{aligned} f_e(X) : g(X) &= (X^6 + X^5 + 0 + X^3 + 0 + X + 0) : (X^3 + X^2 + 0 + 1) = X^3 + \frac{X}{g(X)} \\ &\quad \frac{X^6 + X^5 + 0 + X^3}{0 + 0 + 0 + 0 + 0 + X + 0} \quad (42) \end{aligned}$$

also  $r_f(X) = 0 + X + 0 = S(X) = [S] = [0 \ 1 \ 0]$

### 5. Die Ermittlung des Generatorpolynoms $g(X)$

Die Codewörter haben die Gestalt

$$f(X) = q(X)g(X) = x_0 + x_1X + x_2X^2 \dots + x_{n-1}X^{n-1} \quad (43)$$

Jedes Codewort hat also auch die Wurzeln  $\alpha_1, \alpha_2, \dots, \alpha_m$  des Generatorpolynoms als Wurzeln und damit gilt

$$f(\alpha_i) = 0 = x_0 + x_1 \alpha_i + x_2 \alpha_i^2 \dots + x_{n-1} \alpha_i^{n-1}, \quad (44)$$

oder in Matrixform geschrieben:

$$[1 \ \alpha_1 \ \alpha_1^2 \dots \alpha_1^{n-1}] [x_0 \ x_1 \dots x_{n-1}]^T = 0 \quad (45)$$

Die Codevektoren  $[X] = f(X)$  sind also orthogonal zur Matrix  $H$ , die als Elemente die Wurzeln  $\alpha_i$  von  $g(X)$  enthalten:

$$H = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 \dots \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 \dots \alpha_2^{n-1} \\ \vdots & \vdots & \vdots \\ 1 & \alpha_m & \alpha_m^2 \dots \alpha_m^{n-1} \end{bmatrix} \quad (46)$$

Da aus  $[H]$  entsprechend Gl. (30) die Decodiermatrix  $[B]$  folgt, müssen infolge Gl. (16)  $d - 1 = 2e$  beliebige Spaltenvektoren von  $[H]$  linear unabhängig sein. Das Problem der Konstruktion von Codier- bzw. Decodiermatrizen ist also auf das Auffinden der Wurzeln  $\alpha_i$  verlagert worden, die ein  $g(X)$

ergeben, dass  $X^n - 1$  teilt und die die Forderung nach linearer Unabhängigkeit der Spalten von  $[H]$  erfüllen.

Bose und Chaudhuri haben gezeigt (mit Hilfe Vandermond'schen Determinanten), dass man aus  $[H]$  mindestens  $d - 1$  beliebige Spalten auswählen kann, die linear unabhängig sind, wenn die Codewörter  $f(X)$  über  $GF(q)$  als Wurzeln die Elemente

$$a^{m_0}, a^{m_0+1}, a^{m_0+2}, \dots, a^{m_0+d-2} \quad (47)$$

enthalten, wobei  $a$  ein Element aus dem Erweiterungskörper  $GF(q^m)$  und  $m_0$  eine beliebige ganze Zahl (vorzugsweise  $m_0 = 0$  oder  $1$ ) ist. Die Länge  $n$  der Codewörter ist gleich dem kleinsten gemeinsamen Vielfachen (KGV) der Ordnung  $t$  der Wurzeln  $\beta = \alpha^j$  (d.h.  $\beta^{ti} = \alpha^{j \cdot ti} = 1$ ).

Für Binärcodes erhält man als wichtigsten Fall:

$a$  = primitives Element (= Element der Ordnung  $t = 2^m - 1$ ) aus  $GF(2^m)$ ,  
 $m_0 = 1$  und  $d = 2e + 1$ . Die Codewörter  $f(X)$  und damit  $g(X)$  müssen dann die Wurzeln

$$a, a^2, a^3, \dots, a^{2e} \quad (48)$$

enthalten.

Es existiert zu jedem  $m$  und  $e$  ein binärer Bose-Chaudhuri-Code der Länge  $n = 2^m - 1$ , der  $\leq e$  beliebig verteilte Fehler im Codewort korrigiert und nicht mehr als  $m \cdot e = r$  Prüfstellen benötigt.

Aus den Wurzeln  $\beta_i = a^i$  erhält man das Generatorpolynom  $g(X)$  als kleinstes gemeinsames Vielfaches der Minimalpolynome  $m_i(X)$ , das sind die normierten Polynome [d.h. der Koeffizient der höchsten Potenz in  $m_i(X)$  ist gleich 1] kleinsten Grades, für die  $m_i(\beta_i) = 0$  gilt.

$X^{2^m-1} - 1 = X^n - 1$  besitzt alle  $2^m - 1$  von 0 verschiedenen Elemente aus  $GF(2^m)$  als Wurzeln.  $g(X)$ , nach vorheriger Vorschrift bestimmt, ist also immer Teiler von  $X^n - 1$ , da die Wurzeln von  $g(X)$  Elemente aus  $GF(2^m)$  sind.

Bilden wir z.B. den Erweiterungskörper  $GF(2^m)$  durch  $p(X) = x^3 + 0 + x + 1$  über  $GF(2)$  (irreduzible Polynome können [3] entnommen werden).  $\alpha$  sei die Restklasse, die  $\{X\}$  enthält und ist damit Wurzel von  $p(X)$  sowie gleichzeitig primitives Körperelement aus  $GF(2^m)$ . Die von 0 verschiedenen Körperelemente ergeben sich als Potenzen von  $\alpha$  zu

$$\begin{aligned} \alpha^0 &= 1 + 0 + 0 &= [1 \ 0 \ 0] \\ \alpha^1 &= 0 + \alpha + 0 &= [0 \ 1 \ 1] \\ \alpha^2 &= 0 + 0 + \alpha^2 &= [0 \ 0 \ 1] \\ \alpha^3 &= 1 + \alpha + 0 &= [1 \ 1 \ 0] : X^3 \text{ mod } p(X) = X + 1 \\ \alpha^4 &= 0 + \alpha + \alpha^2 &= [0 \ 1 \ 1] : X^4 \text{ mod } p(X) = X^2 + X \\ \alpha^5 &= 1 + \alpha + \alpha^2 &= [1 \ 1 \ 1] : X^5 \text{ mod } p(X) = x^2 + x + 1 \end{aligned} \quad (49)$$

$$\alpha^6 = 1 + 0 + \alpha^2 = [1 \ 0 \ 1] : X^6 \text{ mod } p(X) = x^2 + 1$$

$$\alpha^7 = 1 + 0 + 0 = \alpha^0 = [1 \ 0 \ 0] : X^7 \text{ mod } p(X) = 1$$

$\alpha$  hat also die Ordnung  $2^3 - 1 = 7$ .

Ein BCH-Code, der  $e = 1$  Fehler korrigiert mit der Blocklänge  $n = 2^m - 1 = 7$ , hat als Wurzeln der Codewörter  $f(X)$  bzw. von  $g(X)$

$$\beta_1 = a \quad \beta_2 = a^2 \quad (50)$$

nach Gl. (48).

Die Minimalpolynome  $m_1(X)$  und  $m_2(X)$  [ $m_1(\beta_1) = 0$ ;  $m_2(\beta_2) = 0$ ] sind irreduzibel über  $GF(2)$ , daher sind z. B. alle Wurzeln von  $m_1(X)$  enthalten in der Folge

$$\beta_1 \beta_1^2 \beta_1^4 \beta_1^8 \dots \beta_1^{2^{r-1}} \quad (51)$$

wenn  $m_1(X)$  vom Grade  $r$  ist. Wählen wir z. B. für  $a = \alpha^3$ , dann hat  $m_1(X)$  die Wurzeln

$$\beta_1 \beta_1^2 \beta_1^4 \quad \left| \quad \beta_1^8 \right. \quad (52)$$

$\alpha^3 \alpha^6 \alpha^{12} = \alpha^5 \quad (\alpha^{24} = \alpha^3 \text{ ist schon vorhanden})$

und ist damit vom Grade  $r = 3$ . Da  $a^2 = \alpha^6$ , die Wurzel von  $m_2(X)$ , bereits in  $m_1(X)$  enthalten ist, folgt

$$g(X) = m_1(X) = (X - \alpha^3)(X - \alpha^6)(X - \alpha^5) \quad (53)$$

Dies ausmultipliziert liefert

$$g(X) = X^3 - (\alpha^3 + \alpha^5 + \alpha^6)X^2 + (\alpha + \alpha^2 + \alpha^4)X - \alpha^{14} \quad (54)$$

Aus der Tabelle der Elemente von  $GF(2^3)$  entnehmen wir

$$\begin{array}{ll} \alpha^3 = 1 + \alpha + 0 & \alpha = 0 + \alpha + 0 \\ \alpha^5 = 1 + \alpha + \alpha^2 & \alpha^2 = 0 + 0 + \alpha^2 \\ + \alpha^6 = 1 + 0 + \alpha^2 & + \alpha^4 = 0 + \alpha + \alpha^2 \\ \hline 1 + 0 + 0 = 1 & 0 + 0 + 0 = 0 \end{array} \quad (55)$$

Also ist

$$g(X) = X^3 - X^2 + 0 - 1 = X^3 + X^2 + 0 + 1 \text{ über } GF(2)$$

Damit zeigte sich, dass das in diesem ganzen Referat verfolgte Beispiel:

1. ein linearer systematischer Code (Gruppencode)
2. ein zyklischer Code
3. ein Hamming Code (dichtgepackter Code)
4. ein BCH-Code

ist.

Dieser Querschnitt aus der Codierungstheorie sollte zeigen, in welcher Weise Galois-Felder und überhaupt die moderne Algebra Anwendung in der Codierungstheorie findet. Verständlicherweise ist gerade das letzte Kapitel nur eine sehr grobe Übersicht, da diese Arbeit sonst zu umfangreich geworden wäre. Zur Vertiefung dieses Kapitels sei auf [3] verwiesen.

Einen Zugang zu den Korrekturverfahren bietet [4] und eine Beurteilung der Fehlerkorrektur aus wirtschaftlicher Sicht wird in [5] versucht.

#### Literatur

- [1] R. Kochendörffer: Einführung in die Algebra. 2. Auflage, Berlin, VEB Deutscher Verlag der Wissenschaften, 1962.
- [2] B. L. Van der Waerden: Algebra. 1. Teil. 5. Auflage. Berlin/Göttingen/Heidelberg, Springer Verlag, 1962.
- [3] W. W. Peterson: Error-correcting codes. New York/London, M.I.T. Press and John Wiley, 1961.
- [4] H. Ohnsorge: Das Eliminieren von Übertragungsfehlern. Techn. Rdsch. 63(1971)28, S. 25...29.
- [5] H. Ohnsorge: Redundant coding and its economical aspects. Eurocon 71, Digest, Palais de Beaulieu, Lausanne, Switzerland, 18...22 october 1971, IEEE Catalog Number 71 C 51-Reg. 8. p. B 6-3/1...B 6-3/2.

#### Adresse des Autors:

Dr. H. Ohnsorge, AEG-Telefunken, Abt. HEIFI, Postfach 830, D-79 Ulm.