Sonderdruck
aus
ARCHIV DER ELEKTRISCHEN ÜBERTRAGUNG

Über die Restfehlerwahrscheinlichkeit zyklischer Binärcodes

von JOACHIM SWOBODA

Über die Restfehlerwahrscheinlichkeit zyklischer Binärcodes

von JOACHIM SWOBODA

Mitteilung aus dem Institut für Nachrichtenvermittlung und Datenverarbeitung
der Technischen Hochschule Stuttgart

(A.E.Ü. **20** [1966], Heft 3, 136–148; eingegangen am 13. Oktober 1965)

DK 621.394.14

Nach einer Einführung in die Theorie zyklischer Binärcodes liefert dieser Beitrag Unterlagen zur Berechnung der Restfehlerwahrscheinlichkeit bei Datenübertragung auf symmetrisch stochastischen Störkanälen.

Die Restfehlerwahrscheinlichkeit p_R ergibt sich allgemein zu $p_R \approx 2^{-k}$ (wobei k die Zahl der Kontrollstellen in Codewörtern der Länge n ist) unabhängig von der Wahrscheinlichkeit p_E falsch übertragener Stellen im Bereich $2k/n \leqq p_E \leqq 1 - (2k/n)$.

Für $p_E < 2k/n$ ist $p_R \lessapprox 2^{-k}$, da für die Zahl $F(w)$ nicht als falsch erkennbarer Fehlermuster mit dem Gewicht w $F(w) \approx \binom{n}{w} \cdot 2^{-k}$ ($w \geqq h$ Hammingdistanz) nachgewiesen werden kann. Dies gilt für viele Typen ungekürzter zyklischer Codes. Dagegen gibt es bei Fire-Codes mehr unerkennbare Fehlermuster von kleinem Gewicht w.

Schwache Verkürzung der Codewortlänge beeinflußt $F(w)/\binom{n}{w} \approx 2^{-k}$ nur unwesentlich. Bei starker Verkürzung sind dagegen grundsätzlich keine allgemeinen Aussagen über $F(w)$ möglich. Durch Verkürzung kann z. B. $F(w)$ für $w = h$ sowohl anwachsen als auch sogar verschwinden. Im letzteren Fall vergrößert sich die Hammingdistanz durch Verkürzung.

Durch Tests auf Rechenmaschinen wurden die theoretischen Aussagen belegt und die der Rechnung nicht zugänglichen Ergebnisse gewonnen.

Following an introduction to the theory of cyclical binary codes this contribution furnishes information for calculating the residual error probability with data transmission on symmetrically stochastic noise channels.

The residual error probability p_R results generally as $p_R \approx 2^{-k}$ (where k the number of check symbols in code words of the length n) independently of the probability p_E of erroneously transmitted symbols in the range $2k/n \leqq p_E \leqq 1 - (2k/n)$.

For $p_E < 2k/n$ there is $p_R \lessapprox 2^{-k}$, since for the number $F(w)$ of error patterns, which cannot be detected as such, and the weight w it can be proven that $F(w) \approx \binom{n}{w} \cdot 2^{-k}$ ($w \geqq h$ Hamming distance). This holds for many types of unshortened cyclical codes. With Fire codes, however, there are more undetectable error patterns of low weight w.

A slight shortening of the code word length affects $F(w)/\binom{n}{w} \approx 2^{-k}$ but insignificantly. With strong shortening, however, no general statements concerning $F(w)$ are basically possible. By shortening it is possible, for instance, that $F(w)$ increases as well as even vanishes for $w = h$. In the latter case the Hamming distance is increased by shortening.

By tests on computers the theoretical statements were proven and those results derived which are not accessible to calculation.

1. Einführung

Für Datenübertragung haben sich binäre Gruppencodes als wirksam zur Sicherung gegen Fehler erwiesen. Von den Gruppencodes lassen sich die zyklischen Binärcodes, die ihrerseits eine Untergruppe der systematischen Binärcodes sind, besonders einfach beschreiben und realisieren (Abschnitt 2). Sie haben deshalb weite Anwendung gefunden.

Die Nachricht liegt als Folge von Binärstellen vor. Es werden bei allen systematischen Codes jeweils m *Nachrichtenstellen* mit k *Prüfstellen* zu einem *Codewort* zusammengefaßt, und der entstandene Block von $n = m + k$ Stellen übertragen. Die Prüfstellen werden aus den Nachrichtenstellen nach einem festen Schema abgeleitet. Die Erfüllung dieses Schemas, die Codevorschrift, läßt sich am Empfangsort kontrollieren, und aufgetretene Fehler können festgestellt werden.

Nicht erkannte Fehler verursachen eine Restfehlerwahrscheinlichkeit. Die Restfehlerwahrscheinlichkeit p_R wird definiert als Wahrscheinlichkeit, daß ein Codewort bei einmaliger Übertragung gestört und als falsch nicht erkannt wird.

Ein bekanntes Merkmal für jeden Code ist die Hammingdistanz h, welche die kleinste Zahl von Fehlerstellen je Codewort angibt, die gerade nicht mehr mit Sicherheit erkannt werden kann. Darüber hinaus erlaubt ein Code auch die Erkennung von Fehlermustern mit mehr Fehlerstellen, jedoch nicht mit Sicherheit. Über die Anteile der nicht als falsch erkennbaren Fehlermuster mit w Fehlerstellen ist noch wenig bekannt. Sie bestimmen aber zusammen mit der Störstatistik des Übertragungskanals die Restfehlerwahrscheinlichkeit.

Man unterscheidet zwei Haupttypen von Störungen auf Binärkanälen:

a) Stochastischer Störkanal

Die Fälschung einer 1-Stelle in eine 0-Stelle und umgekehrt ist gleich wahrscheinlich, *symmetrisch*. Ferner ist das Auftreten einer Fälschung statistisch unabhängig von der Fälschung anderer Stellen (symmetric binary memoryless channel, stochastischer Störkanal).

b) Büschel-Störkanal

Die Fälschung zwischen 1- und 0-Stellen ist ebenfalls symmetrisch. Die Störstellen treten jedoch in

Büscheln auf, d. h. es wechseln störfreie Perioden ab mit Perioden starker Störung ("channel with memory", gemeint ist die Korrelation zwischen den gefälschten Binärstellen).

zu a)

Die Restfehlerwahrscheinlichkeit für den stochastischen Störkanal läßt sich für eine Stellenfehlerwahrscheinlichkeit von $p_E = 0{,}5$ (Index E: error) leicht ermitteln [1], [2], [3]. Es ist $p_R = 2^{-k} - 2^{-n}$. Für beliebiges p_E ergibt sich die Restfehlerwahrscheinlichkeit p_R wie folgt:

Wenn *eine* Stelle mit der Wahrscheinlichkeit p_E gefälscht wird, dann treten in n Codewortstellen genau w gestörte Stellen auf mit der Wahrscheinlichkeit (Binomialverteilung)

$$p(w) = \binom{n}{w} p_E^w (1 - p_E)^{n-w}.$$

Insgesamt gibt es $\binom{n}{w}$ mögliche Fehlermuster mit w Fehlerstellen. Von diesen sei die Zahl der nicht als falsch erkennbaren Muster $F(w)$. Das Verhältnis wird als Reduktionsfaktor $r(w)$ bezeichnet[1] (abweichend von [3]):

$$r(w) = \frac{F(w)}{\binom{n}{w}}.$$

Der Reduktionsfaktor $r(w)$ ist gleich der Wahrscheinlichkeit, daß ein beliebig herausgegriffenes Muster mit w Fehlerstellen nicht als falsch erkennbar ist. Damit ergibt sich p_R als Produkt von $p(w)$ mit $r(w)$, aufsummiert über alle möglichen Fehlerzahlen w,

$$p_R = \sum_{w=0}^{n} p(w)\, r(w) = \tag{1}$$

$$= \sum_{w=0}^{n} \binom{n}{w} p_E^w (1 - p_E)^{n-w} \frac{F(w)}{\binom{n}{w}}. \tag{2}$$

Sinngemäß wird $r(0) = 0$ definiert, da 0 Fehler zu p_R nichts beitragen. Die Gl. (1) verknüpft die Codeeigenschaften mit den Eigenschaften der Störung und liefert die Restfehlerwahrscheinlichkeit. Die Berechnung von p_R bereitet jedoch große Schwierigkeiten, da $r(w)$ nur in Ausnahmefällen explizit angebbar ist.

Ziel dieser Arbeit ist es deshalb, für den stochastischen Störkanal die Reduktionsfunktion $r(w)$ zu bestimmen.

zu b)

Die Berechnung der Restfehlerwahrscheinlichkeit für den Büschelfehlerkanal ist bereits in [4] behandelt worden. Es wurde darin als Sonderfall der Reduktionsfaktor für ein Einzelbüschel in einem Codewort berechnet (Anteil der nicht erkennbaren Fehlerbüschel der Länge b bezogen auf alle Fehlerbüschel der Länge b).

[1] Bei Gruppencodes und damit bei zyklischen Codes ist $F(w)$ gleich der Zahl der *Codewörter* vom Gewicht w (Gewicht ist die Zahl der 1-Stellen in einem Wort, siehe Abschnitt 2). Man könnte damit $r(w)$ auch als bezogene Gewichtsverteilung aller Codewörter eines Code bezeichnen.

2. Eigenschaften zyklischer Binärcodes

Der eingeführte Leser kann diesen Abschnitt überschlagen, da die Theorie der zyklischen Binärcodes aus der einschlägigen Literatur bekannt ist ([6]—[11]). Da jedoch im deutschen Schrifttum wenig über zyklische Codes zu finden ist, wird in diesem Abschnitt eine kurze Einführung gegeben. Sie behandelt insbesondere den Fall der Fehlererkennung.

Ein Codewort besteht aus $m + k = n$ binären Stellen

$$x_1, x_2, \ldots, x_m, x_{m+1}, \ldots, x_{m+k} = x_n,$$

die je den Wert 0 oder 1 annehmen. Die ersten m Stellen sind die Nachricht und können frei gewählt werden, die folgenden k Prüfstellen sind redundant.

Ein zyklischer Code wird durch ein sogenanntes Generatorpolynom beschrieben

$$G(u) = c_k u^k + c_{k-1} u^{k-1} + \cdots + c_1 u^1 + c_0. \tag{3}$$

Der Grad des Polynoms k ist gleich der Zahl der Prüfstellen des Codewortes, die Koeffizienten $c_k, \ldots, c_0$ haben je den Wert 0 oder 1.

Die n Stellen eines Codewortes $x_1, \ldots, x_n$ interpretiert man als Koeffizienten eines Codewortpolynoms $C(u)$ und definiert:

$$C(u) = x_1 u^{n-1} + x_2 u^{n-2} + \cdots + x_{n-1} u^1 + x_n. \tag{4}$$

Definition: Eine Binärfolge $x_1, \ldots, x_n$ ist ein Codewort, wenn das Generatorpolynom $G(u)$ Teiler von $C(u)$ ist. Es ist also die Aufspaltung möglich

$$C(u) = G(u) \cdot Q(u) \quad \ldots \bmod 2. \tag{5}$$

Die Divisionsprozedur muß „modulo 2" ausgeführt werden. Bei dieser gelten die üblichen arithmetischen Gesetze mit den Ausnahmen

$$1 + 1 = 0, \quad +1 = -1 \quad \ldots \bmod 2.$$

Es bezeichnet mod 2 einer Zahl den verbleibenden Rest nach Division dieser Zahl durch 2.

Beispiel für die Division mod 2:

Länge des Codewortes $n = m + k = 4 + 3 = 7$
Generatorpolynom $G(u) = u^3 + u + 1 \triangleq 1011$
Codewortpolynom $C(u) = u^6 + u^3 + u^2 + u^1 \triangleq 1001110$
gemäß Codewortstellen $(x_1\, x_2\, x_3\, x_4\, x_5\, x_6\, x_7) = 1001110$

$C(u)$							:	$G(u)$				=	$Q(u)$			
u^6	u^5	u^4	u^3	u^2	u^1	u^0	:	u^3	u^2	u^1	u^0	=	u^3	u^2	u^1	u^0
1	0	0	1	1	1	0	:	1	0	1	1	=	1	0	1	0
1	0	1	1													
	0	1	0	1												
	0	0	0	0												
		1	0	1	1											
		1	0	1	1											
			0	0	0	0										
			0	0	0	0										
				0	0	0										

Bei der modulo 2-Rechnung braucht wegen $+1 = -1 \pmod 2$ zwischen Addition und Subtraktion

nicht unterschieden zu werden. Das obige Beispiel für die Division geht ohne Rest auf. Damit ist $G(u)$ Teiler von $C(u)$, und die Folge

$$\underbrace{1\ 0\ 0\ 1}_{m=4}\ \vdots\ \underbrace{1\ 1\ 0}_{k=3}$$

ist ein Codewort.

Ferner ist aus dem Beispiel ersichtlich, wie die k Prüfstellen aus den gegebenen m Nachrichtenstellen errechnet werden können: Man setzt in die Prüfstellen zunächst Nullen ein und führt die Division aus. Es wird ein k-stelliger Rest übrigbleiben. Zieht man nun diesen Rest vom Dividenden ab, was einem Ersetzen der letzten k Nullen im Dividenden durch den berechneten Rest entspricht, so ist die erhaltene Folge durch $G(u)$ teilbar und bildet damit ein Codewort.

2.1. *Darstellung des Code durch ein Quersummenschema*

Die Eigenschaften eines zyklischen Code bezüglich der Fehlererkennung sind durch die Länge der Codewörter n und durch das Generatorpolynom $G(u)$ vollständig definiert. Jedoch lassen sich die Eigenschaften der Fehlererkennung besser von einer anderen Darstellungsform, dem sogenannten *Quersummen-Prüfschema*, ablesen. Um dieses Schema zu ermitteln, geht man davon aus, daß das Generatorpolynom $G(u)$ Teiler des Codewortpolynoms $C(u)$ sein muß. Das heißt, es gilt

$$[C(u)]_{\mathrm{mod}\,G(u)} = 0\,, \qquad (6)$$

$$\ldots \mathrm{mod}\ 2$$

$$[x_1 u^{n-1} + x_2 u^{n-2} + \cdots + x_{n-1} u^1 + x_n]_{\mathrm{mod}\,G(u)} = 0. \qquad (7)$$

Die Schreibweise „modulo $G(u)$" bezeichnet den Rest der Division „$C(u)$ geteilt durch $G(u)$", wobei ebenfalls für die Division die modulo 2-Arithmetik anzuwenden ist. Dieser Rest soll nach Gl. (6) Null sein, d. h. $G(u)$ muß Teiler von $C(u)$ sein.

Die Schreibweise von Gl. (6) bzw. Gl. (7) ist aus der sogenannten Polynomrestklassenrechnung bekannt [8], für die Addition und Restbildung vertauscht werden darf. Man erhält damit aus Gl. (7)

$$x_1[u^{n-1}]_{\mathrm{mod}\,G(u)} + x_2[u^{n-2}]_{\mathrm{mod}\,G(u)} + \cdots \quad \ldots \mathrm{mod}\,2$$
$$\cdots + x_{n-1}[u]_{\mathrm{mod}\,G(u)} + x_n[1]_{\mathrm{mod}\,G(u)} = 0\,. \qquad (8)$$

In Gl. (8) sind für die Potenzen von u die Reste der Division zu bilden bezüglich des Generatorpolynoms $G(u)$ des Code. Der Grad von $G(u)$ ist k, die Reste sind also Polynome vom Grade $k-1$ oder kleiner. Ein Koeffizientenvergleich in Gl. (8) für die Potenzen $u^0, u^1, \ldots, u^{k-1}$ der Restpolynome liefert k lineare Gleichungen, denen die Codewortstellen $x_1, \ldots, x_n$ genügen müssen.

Beispiel:

Codewortlänge $n = m + k = 4 + 3 = 7$

Generatorpolynom $G(u) = u^3 + u + 1$

Bedingungsgleichung nach Gl. (8)

$$x_1[u^6]_{\mathrm{mod}\,(u^3+u+1)} + x_2[u^5]_{\mathrm{mod}\,(u^3+u+1)} + \cdots + x_7[1]_{\mathrm{mod}\,(u^3+u+1)} = 0.$$

Berechnung von $[u^0]_{\mathrm{mod}\,(u^3+u+1)} \cdots [u^6]_{\mathrm{mod}\,(u^3+u+1)}$:

u^i	$[u^i]_{\mathrm{mod}\,(u^3+u+1)}$ u^2	u^1	u^0
u^0	.	.	1
u^1	.	1	.
u^2	1	.	.
u^3	.	1	1
u^4	1	1	.
u^5	1	1	1
u^6	1	.	1

z. B.

$u^3 \quad : u^3 + u + 1 = 1$

$u^3 + u + 1$

Rest $u + 1$ ⟵

Der Koeffizientenvergleich führt auf die $k = 3$ Bedingungsgleichungen

$$\begin{aligned} &\text{für } u^2\text{:} && x_1 + x_2 + x_3 + x_5 = 0 \\ &\text{für } u^1\text{:} && x_2 + x_3 + x_4 + x_6 = 0 \quad \ldots \mathrm{mod}\,2 \qquad (9) \\ &\text{für } u^0\text{:} && x_1 + x_2 + x_4 + x_7 = 0 \end{aligned}$$

Gl. (9) schreibt man zweckmäßig in der Form eines Quersummen-Prüfschemas

x_1	x_2	x_3	x_4	x_5	x_6	x_7	
1	1	1	.	1	.	.	
.	1	1	1	.	1	.	Prüfzeile (10)
1	1	.	1	.	.	1	

Prüfspalte

Die mittlere Prüfzeile z. B. fordert, daß die „Quersumme" der Stellen x_2, x_3, x_4, x_6 geradzahlig sein soll, was der Aussage $x_2 + x_3 + x_4 + x_6 = 0 \bmod 2$ entspricht.

2.2. *Prüfschema und Erkennbarkeit von Fehlern*

Bezeichnet man in einem Prüfschema die i-te Prüfspalte mit ihren k Elementen als Spaltenvektor $a_i (i = 1, 2, \ldots, n)$, so erhält das Prüfschema die Form

$$x_1 a_1 + x_2 a_2 + \cdots + x_{n-1} a_{n-1} + x_n a_n = 0 \quad \ldots \mathrm{mod}\,2. \qquad (11)$$

Dabei gelten für die Spalten die üblichen Matrizenregeln, insbesondere für die Summe $a_i + a_j$

$$\begin{pmatrix} a_{i1} \\ a_{i2} \\ \cdot \\ \cdot \\ \cdot \\ a_{ik} \end{pmatrix} + \begin{pmatrix} a_{j1} \\ a_{j2} \\ \cdot \\ \cdot \\ \cdot \\ a_{jk} \end{pmatrix} = \begin{pmatrix} a_{i1} + a_{j1} \\ a_{i2} + a_{j2} \\ \cdot \\ \cdot \\ \cdot \\ a_{ik} + a_{jk} \end{pmatrix} \ldots \mathrm{mod}\,2.$$

Die gefälschten Codewortstellen werden mit

$$x_1', x_2', \ldots, x_n'$$

bezeichnet. Sie ergeben sich aus den ungefälschten Stellen mittels

$$x_i' = x_i + f_i \ldots \mathrm{mod}\,2 \qquad (i = 1, 2, \ldots, n)\,, \qquad (12)$$

wobei $f_i = 0$, wenn die i-te Stelle keinen Fehler enthält,

$f_i = 1$, wenn die i-te Stelle fehlerhaft ist.

Die Folge $f_1, f_2, \ldots, f_n$ wird als *Fehlermuster* bezeichnet. Das gefälschte Codewort $x_1', \ldots, x_n'$ ist nicht als falsch erkennbar, wenn die Codebedingung erfüllt ist, wenn also

$$\begin{aligned} & x_1' a_1 + x_2' a_2 + \cdots + x_n' a_n = 0 \qquad \ldots \bmod 2 \\ & = (x_1 + f_1) a_1 + (x_2 + f_2) a_2 + \cdots + (x_n + f_n) a_n \\ & \qquad\qquad \ldots \bmod 2 \\ & = (x_1 a_1 + x_2 a_2 + \cdots + x_n a_n) + \\ & \quad + (f_1 a_1 + f_2 a_2 + \cdots + f_n a_n) \qquad \ldots \bmod 2 \\ & = f_1 a_1 + f_2 a_2 + \cdots + f_n a_n = 0 \qquad \ldots \bmod 2\,. \quad (13) \end{aligned}$$

Die erste Klammer in der vorletzten Zeile ist Null, da $x_1, x_2, \ldots, x_n$ ein Codewort bildet. Gl. (13) bedeutet: Ein fehlerhaftes Codewort ist genau dann nicht als fehlerhaft erkennbar, wenn die Summe der Prüfspalten, die zu gefälschten Codewortstellen gehören, eine Nullspalte ergibt.

Ferner ist aus Gl. (13) ersichtlich: Die Bedingungsgleichung für ein nicht als falsch erkennbares Fehlermuster $f_1, \ldots, f_n$ stimmt überein mit der Bedingungsgleichung an den Stellen eines Codewortes. Wenn die Fehlerstellen $f_1, \ldots, f_n$ also mit einem Codewort übereinstimmen, so ist dann und nur dann dieses Fehlermuster nicht erkennbar.

2.3. Wichtige Typen zyklischer Binärcodes

2.3.1. Zyklischer Hamming-Code [12]

Das Generatorpolynom $G(u)$ des Hamming-Code ist ein primitives Polynom vom Grad k. Primitive Polynome wurden tabelliert [8] und können nachgeschlagen werden. Die Codewortlänge ist $n = 2^k - 1$. Für ein primitives Polynom $G(u)$ sind die Restpolynome

$$[u^0]_{\bmod G(u)},\ [u^1]_{\bmod G(u)}, \ldots,\ [u^{n-1}]_{\bmod G(u)}$$

paarweise alle verschieden und auch verschieden von Null, so daß nach Abschnitt 2.1 alle Prüfspalten in dem Prüfschema des Code verschieden sind. Von den $2^k - 1$ möglichen Spalten zu je k Elementen mit mindestens einem 1-Element treten alle genau einmal als Prüfspalte auf. Ein Beispiel für den Hamming-Code zeigt das Schema Gl. (10). Damit ist sicher erkennbar jedes Muster mit zwei falschen Stellen in einem Codewort, da die Summe mod 2 von zwei verschiedenen Prüfspalten sicher nicht verschwindet (Abschnitt 2.2).

Nicht erkennbar sind drei Fehlerstellen, falls der dritte Fehler zu jener Prüfspalte gehört, die mit der Summe der Prüfspalten des ersten und zweiten Fehlers übereinstimmt. Die Hammingdistanz des Code, die nicht mit Sicherheit erkennbare kleinste Anzahl von Fehlern, beträgt damit $h = 3$.

Die oben angegebene Codewortlänge von $2^k - 1$ ist die maximale Wortlänge $n_{\max}$. Es ist gegeben $n_{\max}$ als kleinste positive Zahl, für die

$$[u^0]_{\bmod G(u)} = [u^{n_{\max}}]_{\bmod G(u)}$$

gilt.

Die Codewortlänge kann auch beliebig verkürzt werden, ohne daß sich die garantierte Hammingdistanz verringert. Man spricht dann von einem verkürzten Code. Ebenso wie der Hamming-Code dürfen alle folgenden Codes verkürzt werden.

2.3.2. Abramson-Code [10]

Das Generatorpolynom $G(u) = G_1(u)\,(u + 1)$ besteht aus zwei Faktoren. $G_1(u)$ ist primitiv und vom Grad k_1. Der Grad von $G(u)$ ist $k = k_1 + 1$. Die ungekürzte Codewortlänge ergibt sich zu

$$n = 2^{k_1} - 1 = 2^{k-1} - 1\,.$$

Das Prüfschema des Abramson-Code baut man zur besseren Übersicht aus zwei Teilen auf. Da $G(u)$ Faktor des Codewortpolynoms $C(u)$ ist, sind $G_1(u)$ wie auch $(u + 1)$ Faktor von $C(u)$. Aus der ersten Bedingung, $[C(u)]_{\bmod G_1(u)} = 0$, erhält man k_1 Zeilen für das Prüfschema, das mit jenem eines Hamming-Code gleicher Codewortlänge übereinstimmt. Die zweite Bedingung, $[C(u)]_{\bmod (u+1)} = 0$, liefert eine weitere Prüfzeile, die durchgehend mit 1 besetzt ist:

$$[u^0]_{\bmod (u+1)} = [u^1]_{\bmod (u+1)} = \cdots$$
$$\cdots = [u^{n-1}]_{\bmod (u+1)} = 1.$$

Beispiel:

$$G(u) = (u^3 + u + 1)\,(u + 1)\,,$$
$$n = 2^{4-1} - 1 = 7$$

x_1	x_2	x_3	x_4	x_5	x_6	x_7
1	1	1	.	1	.	.
.	1	1	1	.	1	.
1	1	.	1	.	.	1
1	1	1	1	1	1	1

Im Abramson-Code sind zwei Fehler sicher erkennbar. Darüber hinaus werden allgemein ungeradzahlig viele Fehlerstellen sicher erkannt, da die zeilenweise Summe mod 2 von ungeradzahlig vielen Prüfspalten in der untersten Position eine 1 liefert; die Spaltensumme ist von Null verschieden. Damit sind bis zu drei Fehler sicher erkennbar, dagegen vier Fehler nicht mit Sicherheit. Die Hammingdistanz des Abramson-Code beträgt $h = 4$.

2.3.3. Fire-Code [13]

Das Generatorpolynom $G(u) = G_1(u)\,(u^{k_2} + 1)$ besteht aus zwei Faktoren. $G_1(u)$ ist primitiv und vom Grad k_1. Der Grad von $G(u)$ ist $k = k_1 + k_2$. Die beiden Zahlen $2^{k_1} - 1$ und k_2 sollen teilerfremd sein. Die ungekürzte Codewortlänge ergibt sich zu $n = (2^{k_1} - 1)\,k_2$.

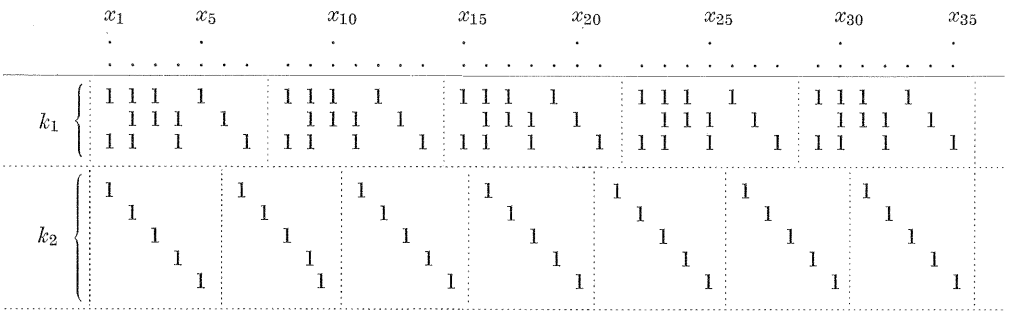
Das Prüfschema des Fire-Code läßt sich analog wie beim Abramson-Code aus den beiden Bedingungen

$$[C(u)]_{\bmod G_1(u)} = 0\,,$$
$$[C(u)]_{\bmod (u^{k_2}+1)} = 0$$

gewinnen.

Beispiel:

$$G(u) = (u^3 + u + 1)\,(u^5 + 1)$$
$$n = (2^3 - 1) \cdot 5 = 35$$



In dem Prüfschema des Fire-Code wiederholt sich im oberen Teil das Prüfschema eines Hamming-Code vom Grad k_1 in k_2-facher Vielfalt. Im unteren Teil wiederholen sich die ersten k_2 Teilspalten $(2^{k_1} - 1)$-fach. Bemerkenswert ist, daß über den Einsen einer festgewählten „k_2-Prüfzeile" die „k_1-Prüfspalten" alle verschieden sind, und jede mögliche k_1-Prüfspalte genau einmal auftritt.

Erkennbar sind alle Muster mit zwei Fehlern, da alle vollständigen Prüfspalten paarweise verschieden sind. Ferner sind erkennbar alle Muster mit drei Fehlern, da die Summe mod 2 von drei Prüfspalten in den unteren k_2 Positionen mindestens eine Eins enthält und damit nicht zu Null wird. Der Fire-Code hat trotz seiner höheren Zahl an Prüfstellen auch nur eine Hammingdistanz von $h = 4$. Der höhere Aufwand ist durch die Fähigkeiten gegenüber Büschelfehlern bedingt (es können zwei Fehlerbüschel von der Gesamtlänge $k_2 + 1$ mit Sicherheit erkannt werden).

2.3.4. Bose-Chauduri-Code

Das Generatorpolynom

$$G(u) = G_1(u)\, G_2(u) \ldots G_e(u)$$

besteht aus e Faktoren. $G_1(u)$ ist primitiv und vom Grad k_1. Die anderen Teilpolynome werden aus $G_1(u)$ berechnet, worauf hier nicht näher eingegangen wird. Der Grad der Teilpolynome $G_2(u) \ldots G_e(u)$ ist ebenfalls k_1 oder kleiner als k_1. Damit ergibt sich der Grad von $G(u)$ zu

$$k \leqq e\, k_1 = e \operatorname{ld}(n + 1).$$

Die ungekürzte Codewortlänge ist $n = 2^{k_1} - 1$.

Sicher erkennbar sind $2e$ Fehler, womit sich die Hammingdistanz zu $h = 2e + 1$ ergibt.

3. Restfehlerwahrscheinlichkeit für den erweiterten Bereich $p_E = 2\,k/n \ldots 1 - (2\,k/n)$

Bei einer Schrittfehlerwahrscheinlichkeit von $p_E = 0{,}5$ entstehen durch Fälschung alle 2^n möglichen Zeichen mit gleicher Wahrscheinlichkeit. Die Restfehlerwahrscheinlichkeit ergibt sich für diesen Sonderfall als Verhältnis aller $2^m - 1$ möglichen Codewörter (ausgenommen das gestörte Ausgangscodewort) zu allen 2^n möglichen Zeichen mit je n Stellen [1]. Damit wird $p_R = 2^{-k} - 2^{-n}$.

Für Codes, bei denen $m = n - k \gg 1$ ist, ergibt sich für $p_E = 0{,}5$ die Näherung

$$p_R \approx 2^{-k} \text{ für } m = n - k \gg 1 \text{ und } p_E = 0{,}5. \quad (14)$$

Es kann jedoch gezeigt werden, daß sich p_R fast nicht ändert, wenn p_E von 0,5 verschieden ist. Die Herleitung im Anhang 1 ergibt für Gl. (14) den erweiterten Gültigkeitsbereich

$$p_R \approx 2^{-k} \quad \text{für} \quad 2\,k/n \leqq p_E \leqq 1 - (2\,k/n). \quad (15)$$

Nach Gl. (15) gilt diese Restfehlerwahrscheinlichkeit für einen um so größeren Bereich der Stellenfehlerwahrscheinlichkeit p_E, je redundanzärmer der Code ist. Die Grenze $2k/n$ ergibt sich in der Herleitung aus der Forderung, daß p_R in dem Intervall

$$p_R = 2^{-k}(1 \pm 0{,}02\,k) \quad (16)$$

liegen soll.

Gl. (15) gilt allgemein für jeden zyklischen Code und für alle üblichen systematischen Codes.

4. Ermittlung der Reduktionsfunktion

4.1. Übersicht

Eine genauere Kenntnis der Reduktionsfunktion $r(w)$ ist nötig für die Berechnung der Restfehlerwahrscheinlichkeit p_R bei einer Stellenfehlerwahrscheinlichkeit $p_E < 2k/n$.

Der Reduktionsfaktor $r(w)$ wurde definiert als die Zahl $F(w)$ nicht erkennbarer Fehlermuster vom Gewicht w (w ist die Zahl der falschen Stellen im Fehlermuster) geteilt durch die Zahl $\binom{n}{w}$ aller möglichen Fehlermuster vom Gewicht w in n Stellen. Die Gesamtheit aller Reduktionsfaktoren $r(w)$, $1 \leqq w \leqq n$, wird als Reduktionsfunktion bezeichnet. Für einen festen Wert w heißt $r(w)$ Reduktionsfaktor.

Die Reduktionsfunktion läßt sich nur für wenige Fälle explizit angeben. Allgemein gilt

$$r(w) = 0 \quad \text{für} \quad w < h, \quad (17)$$

da Fehlermuster von geringerem Gewicht als die Hammingdistanz sicher erkennbar sind.

Folgende weitere Angaben über die Reduktionsfunktion sind möglich:

4.1.1. Für einige ungekürzte Codes (Abschnitt 2.3.1) läßt sich die Reduktionsfunktion auf kombinatorischem Wege vollständig berechnen, nämlich für

gewöhnliche Quersummen-Codes (nur ein Parity-Bit je Codewort),
Hamming-Codes,
Abramson-Codes.

Für den Fire-Code (Hammingdistanz $h = 4$) läßt sich nur der Reduktionsfaktor $r(w) = r(4)$ mit erträglichem Aufwand kombinatorisch berechnen (Abschnitt 4.2).

4.1.2. Die Restfehlerwahrscheinlichkeit fast beliebiger Codes ist aus Abschnitt 3 bekannt für eine Stellenfehlerwahrscheinlichkeit

$$2k/n \leqq p_E \leqq 1 - (2k/n).$$

Davon läßt sich rückwärts auf die Reduktionsfunktion $r(w)$ im Bereich $2k \leqq w \leqq n - 2k$ schließen (siehe Abschnitt 4.3).

4.1.3. Die kombinatorische Berechnung von $r(w)$ außerhalb $2k \leqq w \leqq n - 2k$ versagt für viele andere Codes, auf jeden Fall für *gekürzte* zyklische Codes. In diesen Fällen muß man Testverfahren zu Hilfe nehmen, um den noch unbekannten Bereich der Reduktionsfunktion $r(w)$ für $w < 2k$ zu schließen. Große Fehlerzahlen, $w > n - 2k$, für die Reduktionsfunktion interessieren weniger, da sogar für die maximale Störung, die bei der Stellenfehlerwahrscheinlichkeit von $p_E = 0{,}5$ auftritt, Fehlermuster von so hohem Gewicht nur einen verschwindenden Anteil ausmachen.

Es gibt folgende zwei Testverfahren, die beide vom Verfasser herangezogen wurden (Abschnitt 4.4).

a) Statistische Testmethode (Monte-Carlo-Verfahren)

Auf einem elektronischen Rechner werden Zufallsmuster von genau w Fehlern in n Stellen erzeugt, wobei jedes der $\binom{n}{w}$ möglichen Muster gleich wahrscheinlich auftritt. Jedes Fehlermuster wird auf Erkennbarkeit geprüft. Der Anteil der nicht als falsch erkennbaren Muster an allen untersuchten Mustern ist der Schätzwert für den Reduktionsfaktor $r(w)$.

b) Systematische Testmethode

Es werden systematisch alle $\binom{n}{w}$ möglichen Muster von w Fehlern in n Stellen erzeugt und ihre Erkennbarkeit geprüft. Dieses Verfahren liefert den exakten Wert für $r(w)$. Da dieses Testverfahren durch einen großen Aufwand an Rechenzeit gekennzeichnet ist, wurde hierfür ein kleiner Spezialrechner gebaut.

Kenndaten des Spezialrechners:

Codewortlänge	$n \leqq 1023$,
Zahl der Prüfstellen	$k \leqq 21$,
Generatorpolynom	beliebig (bis zum angegebenen Grad k),
Gewicht der Fehlermuster	$w \leqq 10$ (16),
Arbeitsgeschwindigkeit	etwa 10^4 Codewortstellen pro Sekunde.

4.2. Berechnung der Reduktionsfunktion für einige ungekürzte Codes

4.2.1. Gewöhnlicher Quersummen-Code

Bei diesem Code ergänzt $k = 1$ Prüfstelle das ganze Codewort von m auf $n = m + k$ Stellen so, daß es eine gerade Anzahl von 1-Stellen enthält. Alle Zeichen mit gerader Quersumme sind demnach Codewörter. Daher sind alle Fehlermuster mit ungeradem Gewicht erkennbar und alle Fehlermuster mit geradem Gewicht nicht erkennbar.

Für die Reduktionsfunktion folgt

$$\begin{aligned} r(w) &= 0 \quad \text{für} \quad w = \text{ungerade}, \\ r(w) &= 1 \quad \text{für} \quad w \geqq 2 \text{ und gerade}. \end{aligned} \tag{18}$$

Faßt man jeweils zwei benachbarte Reduktionsfaktoren zusammen, so ergibt sich im Mittel

$$r(w) = 0{,}5 = 2^{-1} = 2^{-k}.$$

4.2.2. Hamming-Code

Für den ungekürzten Hamming-Code läßt sich die Reduktionsfunktion leicht angeben, da für diesen die Anzahl der Codewörter mit dem Gewicht w bekannt ist ([8], S. 68). Die Rekursionsformel aus [8] lautet in den hier verwendeten Symbolen

$$F(w) = \frac{1}{w}\left[\binom{n}{w-1} - F(w-1) - (n - w + 2)\,F(w-2)\right], \tag{19}$$

wobei $F(1) = 0$, $F(2) = 0$, $n = 2^k - 1$.

Die Rekursionsformel Gl. (19) läßt sich mittels $r(w) = F(w)\Big/\binom{n}{w}$ umschreiben in eine Rekursionsformel für die Reduktionsfunktion

$$r(w) = \frac{1}{n - w + 1} \times \left[1 - r(w-1) - (w-1)\,r(w-2)\right]. \tag{20}$$

Die ersten Werte lauten

$$\begin{aligned} r(1) &= r(2) = 0, \\ r(3) &= r(4) = \frac{1}{n-2}, \\ r(5) &= r(6) = \frac{n-7}{(n-2)(n-4)}, \\ &\ldots \end{aligned}$$

Für das Beispiel $n = 2^k - 1 = 2^5 - 1 = 31$ ist die Reduktionsfunktion in Bild 1 dargestellt, wobei $r(w)$ auf 2^{-k} bezogen wurde.

Die Reduktionsfunktion ist symmetrisch

$$r(w) = r(n - w) \quad \text{für} \quad 0 \neq w \neq n \tag{21}$$

außer $r(0) = 0$, $r(n) = 1$.

Ferner ist auffällig die paarweise Gleichheit von $r(w)$.

Um für größere Werte von w das Lösen der Rekursionsgleichung (20) zu ersparen, kann man eine obere und untere Schranke für $r(w)$ aufstellen. Eine

obere Schranke erhält man, indem in Gl. (20) die negativen Glieder weggelassen werden. Eine untere Schranke ergibt sich durch Einsetzen der oberen Schranke von $r(w-1)$ und $r(w-2)$ in Gl. (20):

$$\frac{1}{n-w+1}\left(1-\frac{w}{n-w+1}\right) < r(w) < \frac{1}{n-w+1}$$

oder mit $n = 2^k - 1$ (22)

$$\frac{1}{2^k-w}\left(1-\frac{w}{2^k-w}\right) < r(w) < \frac{1}{2^k-w}.$$

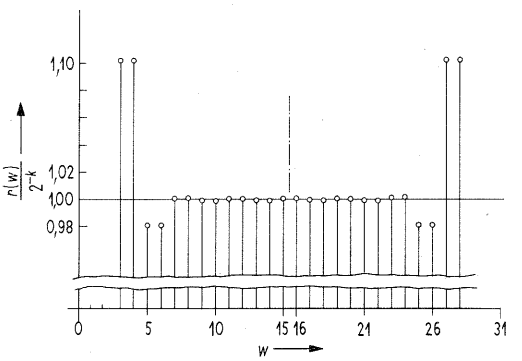


Bild 1. Berechnete Reduktionsfunktion des Hamming-Code mit $n = 31$ Stellen und $k = 5$ Prüfstellen. $r(w)$ ist der Anteil nicht als falsch erkennbarer Fehlermuster vom Gewicht w. Das Bild zeigt die Abweichung gegenüber 2^{-k}. Man beachte den unterbrochenen Ordinatenmaßstab.

Die Gl. (22) grenzt die Reduktionsfunktion $r(w)$ um so schärfer auf den Wert $r(w) = 2^{-k}$ ein, je größer die Codewortlänge $n = 2^k - 1$ gegenüber w ist. Gl. (22) soll in dem Bereich $h = 3 \leqq w < 2k$ herangezogen werden. Für größeres Fehlergewicht w, d. h. $2k \leqq w \leqq n - 2k$, wird die Näherung $r(w) \approx 2^{-k}$ allgemein noch im Abschnitt 4.3 nachgewiesen. Damit ist $r(w) \approx 2^{-k}$ für den Bereich $3 \leqq w \leqq n - 2k$ sichergestellt. Schließlich kann mittels der Symmetriebeziehung Gl. (21) der Gültigkeitsbereich nach oben von $w \leqq n - 2k$ auf $w \leqq n - h$ ausgedehnt werden.

Damit darf für die Reduktionsfunktion des Hamming-Code geschrieben werden

$$\begin{aligned} r(w) &\approx 2^{-k} \quad \text{für} \quad 3 \leqq w \leqq n-3, \\ r(w) &= 0 \qquad \text{für} \qquad w < 3. \end{aligned} \tag{23}$$

Es ist wichtig festzustellen, daß die Restfehlerwahrscheinlichkeit p_R den Wert 2^{-k} weder für starke Störung und schon gar nicht für schwache Störung überschreiten kann. Würde für eine Datenübertragung ein Hamming-Code mit z. B. $k = 20$ Prüfstellen benutzt werden, so wäre die Restfehlerwahrscheinlichkeit maximal

$$p_R \leqq 2^{-k} = 2^{-20} \approx 10^{-6}.$$

4.2.3 Abramson-Code

In dem Quersummen-Prüfschema eines Abramson-Code (Abschnitt 2.3.2) erfaßt eine der k Prüfgleichungen *alle* Codewortstellen. Dies hat zur Folge, daß alle Codewörter geradzahliges Gewicht haben und Fehlermuster mit ungeradem Gewicht sicher erkennbar sind. Damit wird

$$r(w) = 0 \quad \text{für} \quad w = \text{ungerade}. \tag{24}$$

Die restlichen $k - 1$ Prüfgleichungen bilden ein Prüfschema, das mit jenem eines Hamming-Code mit gleicher Zahl von $n = 2^{k-1} - 1$ Codewortstellen übereinstimmt. Für Fehlermuster von geradem Gewicht gelten daher die gleichen Reduktionsfaktoren wie für den Hamming-Code gleicher Codewortlänge und mit $k_1 = k - 1$ Prüfgleichungen.

Es folgt für die Reduktionsfunktion

$$r(w) = 0 \qquad \text{für} \quad w = \text{ungerade}, \tag{25}$$

$$r(w) \approx 2^{-k+1} = 2 \cdot 2^{-k} \quad \text{für} \quad 4 \leqq w_{\text{gerade}} \leqq n - 3.$$

Die Reduktionsfunktion für gerade Fehlerzahl nimmt also gegenüber 2^{-k} den doppelten Wert an. Faßt man jedoch zwei in w benachbarte Werte von $r(w)$ zusammen, so ergibt sich für die Reduktionsfunktion im Mittel ebenfalls wieder 2^{-k}.

4.2.4. Fire-Code

Ebenso wie beim Abramson-Code ist auch bei dem für die Sicherung gegen Büschelfehler entwickelten Fire-Code jedes Fehlermuster mit ungeradem Gewicht erkennbar. Man kann dies leicht am Prüfschema des Fire-Code ablesen (Abschnitt 2.3.3): Bildet man die Summe der k_2 Prüfgleichungen, so erhält man *eine* Prüfgleichung, die alle Codewortstellen erfaßt. Diese zeigt aber jedes Fehlermuster mit ungeradem Gewicht an. Also

$$r(w) = 0 \quad \text{für} \quad w = \text{ungerade}. \tag{26}$$

Die verbleibenden Reduktionsfaktoren für gerade Fehlerzahlen konnten allgemein nicht berechnet werden. Jedoch liefert der Reduktionsfaktor für $w = h = 4$ schon ein sehr interessantes Ergebnis. Im Anhang 2 wird die Zahl der nicht als falsch erkennbaren Fehlermuster mit $w = 4$ Fehlern hergeleitet:

$$F(4) = \frac{1}{4!} k_2 (2^{k_1} - 1)(2^{k_1} - 2) \times \tag{27}$$
$$\times [(2^{k_1} - 4) + 3(k_2 - 1)(2^{k_1} - 2)].$$

Mit der Näherung $2^{k_1} - 1 \gg 1$ ergibt sich daraus der Reduktionsfaktor

$$r(4) \approx \frac{(3k_2 - 2) \cdot 2^{k_2}}{2 k_2^3} \cdot 2 \cdot 2^{-k}. \tag{28}$$

In Gl. (28) ist $k = k_1 + k_2$ der Grad des vollständigen Generatorpolynoms und k_2 der Grad des Polynomanteiles $(u^{k_2} + 1)$. Je größer k_2 gewählt wird, um so größer sind auch die Sicherungseigenschaften des Code gegenüber Fehlerbüscheln.

Bild 2 zeigt den auf $2 \cdot 2^{-k}$ bezogenen Reduktionsfaktor nach Gl. (28), der in der Näherung nur eine Funktion von k_2 ist. Bild 2 gibt an, um wieviel mal größer der Reduktionsfaktor $r(4)$ des Fire-Code ist gegenüber dem Reduktionsfaktor $r(4)$ des Abramson-Code, wobei gleicher Grad des Generatorpolynoms vorausgesetzt ist. Es ist aus Bild 2 ersichtlich, daß für $w = 4$ die verbesserten Sicherungseigen-

schaften gegenüber Büschelfehlern (größeres k_2 bei $k = k_1 + k_2 = \text{const}$) sehr empfindlich bezahlt werden müssen mit einer Vergrößerung der Restfehlerwahrscheinlichkeit bei dem hier untersuchten stochastischen Störkanal.

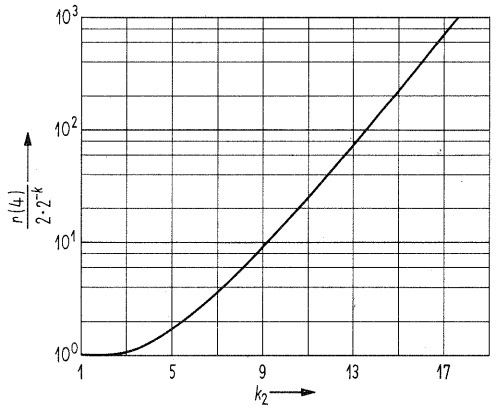


Bild 2. Berechneter Reduktionsfaktor $r(4)$ bezogen auf $2 \cdot 2^{-k}$ für einen beliebigen Fire-Code mit einem Generatorpolynom $G(u) = G_1(u)\,(u^{k_2} + 1)$. Der Abszissenwert k_2 bestimmt die Fähigkeit des Fire-Code gegenüber Büschelfehlern. Der Grad von $G_1(u)$ ist k_1, der Grad von $G(u)$ ist $k = k_1 + k_2$. Für den Grenzwert $k_2 = 1$ liegt ein Abramson-Code vor.

Reduktionsfaktoren für Fehlergewichte $w > 4$ sind beim Fire-Code auf kombinatorischem Wege nur äußerst aufwendig zu erhalten. Die kombinatorische Methode versagt sogar generell, wenn man gekürzte Codes untersuchen will. Es helfen in diesem Fall nur noch Monte-Carlo-Testmethoden und systematische Testmethoden weiter.

4.3. Berechnung der Reduktionsfunktion beliebiger Codes für den Bereich $w = 2k \ldots n - 2k$

Die Ergebnisse von Abschnitt 4.2 lassen für die Reduktionsfunktion vieler Codes einen Wert $\approx 2^{-k}$ in einem weiten Bereich vermuten. Tatsächlich folgt aus dem Ergebnis von Abschnitt 3 ($p_R \approx 2^{-k}$ für $2k/n \leqq p_E \leqq 1 - (2k/n)$) für die Reduktionsfunktion $r(w)$, daß sie in einem weiten Bereich von w konstant den Wert $\approx 2^{-k}$ annimmt (Herleitung siehe Anhang 3):

$$r(w) = 2^{-k} \quad \text{für} \quad 2k \leqq w \leqq n - 2k\,. \qquad (29)$$

Dieses Ergebnis soll an Hand von Bild 3 näher diskutiert werden.

In Bild 3b ist die Hüllkurve der Fehlerwahrscheinlichkeiten

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

für den Fall $n = 100$, $p_E = 0{,}5$ (———) und $p_E = 0{,}25$ (— — —) dargestellt. Der Erwartungswert der Verteilung ist $n p_E$, die Streuung ist

$$\sigma = \sqrt{p_E (1 - p_E)\, n}\,.$$

Bild 3a zeigt die Hüllkurve der Reduktionsfunktion.

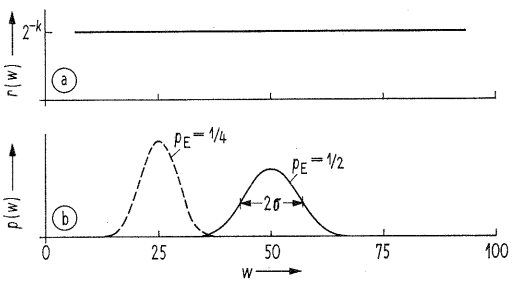


Bild 3. Hüllkurven für die Reduktionsfunktion $r(w)$ und die Binomialverteilung der Fehlerwahrscheinlichkeiten $p(w)$. Mit $p(w)$ treten Fehlermuster vom Gewicht w auf in $n = 100$ Stellen bei einer Stellenfehlerwahrscheinlichkeit von $p_E = 1/2$ (———) bzw. $p_E = 1/4$ (— — —).

Die Funktion $r(w)$ trägt offenbar zur Restfehlerwahrscheinlichkeit

$$p_R = \sum_{w=0}^{n} p(w)\, r(w)$$

nur über jenen Abschnitten der w-Achse wesentlich bei, innerhalb derer die Glockenkurven $p(w)$-Werte liefern, die nicht vernachlässigbar klein sind. Wenn $r(w)$ nicht so glatt verläuft, wie in Bild 3a als Möglichkeit gezeichnet, sondern eine gewisse „Welligkeit" aufweist, so wird dies auf $p_R(p_E)$ nur einen geringen Einfluß haben, solange die „Welligkeitsperioden" kurz sind gegenüber der Breite 2σ der $p(w)$-Verteilungen.

Eine solche Welligkeit kann tatsächlich auftreten und zwar aus folgendem Grund: Die Herleitung von Gl. (29) erfolgte unter der Näherungsannahme, daß $p_R(p_E) = 2^{-k}$ für einen gewissen Bereich von p_E exakt gilt. In Wirklichkeit hängt aber $p_R \approx 2^{-k}$ nur näherungsweise nicht von p_E ab. Diese Welligkeit findet sich bei Codes, welche nur Worte mit geradzahligen Gewichten haben (gewöhnlicher Quersummen-Code, Abramson-Code, Fire-Code). Für diese Codes ist

$$r(w_{\text{ungerade}}) = 0 \quad \text{und} \quad r(w_{\text{gerade}}) \approx 2 \cdot 2^{-k}\,,$$

so daß Gl. (29) dann nur im Mittel für zwei benachbarte Reduktionsfaktoren erfüllt ist.

4.4. Bestimmung der Reduktionsfunktion mit Hilfe von Testverfahren für den Bereich $w < 2k$

Die Ergebnisse, die in diesem Abschnitt dargestellt sind, wurden aus systematischen und statistischen Testmethoden gewonnen. Es wurden Codes und Fehlerbereiche untersucht, die der Berechnung nicht zugänglich sind. Die Reduktionsfunktion muß punktweise für jeden Wert w ermittelt werden, indem ein Codewort entweder systematisch mit allen möglichen Fehlermustern von w Fehlern in n Stellen oder mit sehr vielen statistisch ausgewählten Zufallsmustern vom Gewicht w gestört wird.

Für jedes Fehlermuster wird dessen Erkennbarkeit geprüft. Der Anteil der nicht erkennbaren Fehlermuster an allen geprüften Mustern vom Gewicht w ist der Reduktionsfaktor $r(w)$.

Die statistische Methode bringt es mit sich, daß die einzelnen Reduktionsfaktoren nicht exakt angegeben werden können. In den Diagrammen mit statistisch ermittelten Ergebnissen sind deshalb Vertrauensintervalle angegeben, innerhalb derer $r(w)$ mit 95% Sicherheit liegt.

Jede Reduktionsfunktion gilt zunächst nur für den untersuchten Code, der durch seine Codewortlänge n und das Generatorpolynom $G(u)$ gegeben ist. Um einen Überblick über die Reduktionsfunktionen verschiedener Codes nach Typ und Wortlänge zu erhalten, mußten Tests in großem Umfange durchgeführt werden. Im folgenden wird zwischen ungekürzten Codes und gekürzten Codes unterschieden (siehe Abschnitt 2.3).

4.4.1. Ungekürzte Codes

Für ungekürzte Codes konnte die Reduktionsfunktion auf kombinatorischem Wege nicht ermittelt werden für Fire-Codes, ausgenommen $r(w)$ für $w = h = 4$, und für Bose-Chauduri-Codes gar nicht. Nur diese zwei Codes müssen hier betrachtet werden.

Für den *Fire-Code* sind in Bild 4 zwei Beispiele der Reduktionsfunktion dargestellt, wobei auf $2 \cdot 2^{-k}$ bezogen wurde. Die Reduktionsfunktionen gelten für

a) $G(u) = (u^3 + u + 1)(u^5 + 1)$, $n = 35$,

b) $G(u) = (u^3 + u + 1)(u^9 + 1)$, $n = 63$;

($h = 4$ für alle Fire-Codes).

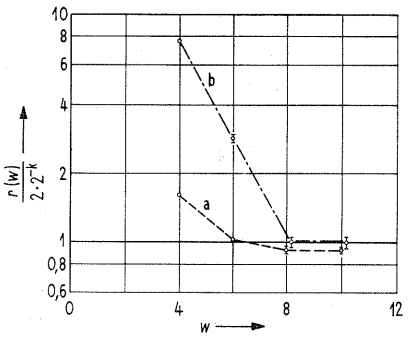


Bild 4. Durch Test ermittelte Reduktionsfunktion $r(w)$ bezogen auf $2 \cdot 2^{-k}$ zweier ungekürzter Fire-Codes mit den Generatorpolynomen
a) $G(u) = (u^3 + u + 1)(u^5 + 1)$, $n = 35$, $k = 8$,
b) $G(u) = (u^3 + u + 1)(u^9 + 1)$, $n = 63$, $k = 12$.
Auffällig ist das Ansteigen von $r(4)$ für den Code b von hohem Grad k_2 des Polynomteiles $(u^{k_2} + 1)$.

Das Ansteigen der Reduktionsfunktion für kleine Fehlerzahlen w fällt auf. Der Anstieg ist um so stärker, je größer der Grad k_2 des zweiten Polynomanteiles im Generatorpolynom $G(u)$ ist. Der Reduktionsfaktor für den Sonderfall $w = 4$ stimmt mit dem Rechenwert aus Gl. (27) exakt überein, für den der Anstieg mit wachsendem Grad k_2 bereits gezeigt wurde (siehe auch Bild 2).

Nach größeren Fehlerzahlen w hin nähert sich die Reduktionsfunktion $r(w)$ von oben dem Wert $2 \cdot 2^{-k}$ (w ungerade). Dies bestätigt die Aussage über die Reduktionsfunktion für beliebige Codes nach Gl. (29) ($r(w) \approx 2^{-k}$ für $2k \leqq w \leqq n - 2k$). Da für den Fire-Code alle Fehlermuster mit ungeradem Gewicht erkennbar sind, streben in Bild 4 die über zwei benachbarte Werte w gemittelten Reduktionsfunktionen dem Wert 2^{-k} zu (vgl. Abschnitt 4.2.4).

Für den *Bose-Chauduri-Code* sind in Bild 5 drei Beispiele der Reduktionsfunktion dargestellt, wobei auf 2^{-k} bezogen wurde. Die Reduktionsfunktionen gelten für

a) $G(u) = (u^4 + u + 1)(u^4 + u^3 + u^2 + u + 1)$, $n = 15$,

b) $G(u) = (u^5 + u^2 + 1)(u^5 + u^4 + u^3 + u^2 + 1)$, $n = 31$,

c) $G(u) = (u^6 + u + 1)(u^6 + u^4 + u^2 + u + 1)$, $n = 63$.

Alle drei Codes haben eine Hammingdistanz von $h = 5$, bis zu $w = 4$ Fehler sind also sicher erkennbar.

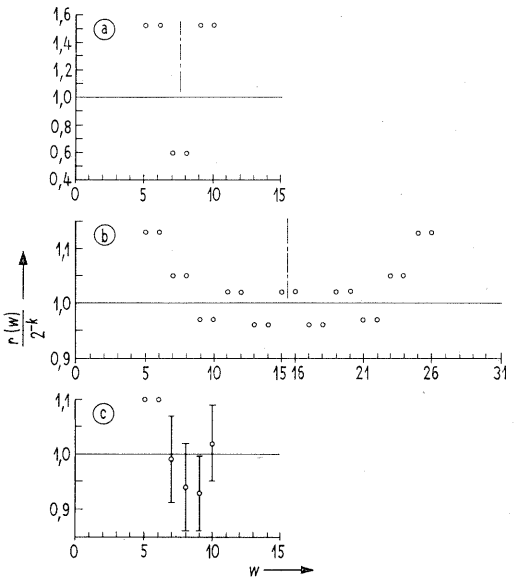


Bild 5. Durch Test ermittelte Reduktionsfunktionen $r(w)$ bezogen auf 2^{-k} dreier ungekürzter Bose-Chauduri-Codes mit den Generatorpolynomen
a) $G(u) = (u^4 + u + 1)(u^4 + u^3 + u^2 + u + 1)$, $n = 15$, $k = 8$,
b) $G(u) = (u^5 + u^2 + 1)(u^5 + u^4 + u^3 + u^2 + 1)$, $n = 31$, $k = 10$,
c) $G(u) = (u^6 + u + 1)(u^6 + u^4 + u^2 + u + 1)$, $n = 63$, $k = 12$.
Die Abweichung gegenüber 2^{-k} verringert sich mit zunehmender Länge der Codes. Auffällig ist die paarweise exakte Gleichheit der Reduktionsfaktoren.

Die Ergebnisse zeigen, daß für den Bose-Chauduri-Code die Reduktionsfunktion $r(w)$ in dem gesamten Bereich $h \leqq w \leqq n - h$ bei dem kurzen Code ($n = 15$) durch 2^{-k} weniger gut angenähert wird. Bei langen Codes ($n = 31$, 63) wird die Annäherung zunehmend besser. Außerhalb des Bereiches $h \leqq w \leqq n - h$ ist $r(w) = 0$, ausgenommen $r(n) = 1$. Ferner ist die Reduktionsfunktion wie bei dem Hamming-Code symmetrisch bezüglich

$$w = n/2 .$$

4.4.2. Gekürzte Codes

Um den Einfluß der Verkürzung der Codewortlänge zu untersuchen, werden Reduktionsfunktionen $r(w)$ für ein festes Generatorpolynom, aber unterschiedliche Codewortlängen ermittelt.

Bild 6 zeigt Beispiele der Reduktionsfunktion für einen *Abramson-Code* mit dem festen Generatorpolynom

$$G(u) = (u^8 + u^7 + u^2 + u + 1)(u + 1).$$

Die Codewortlängen sind

a) $n = n_{\max} = 255$,
b) $n = 200$,
c) $n = 100$,
} verkürzt.

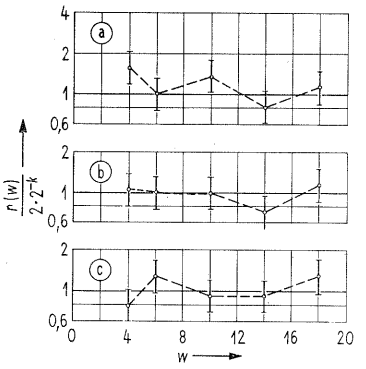


Bild 6. Durch Test ermittelte Reduktionsfunktionen $r(w)$ bezogen auf $2 \cdot 2^{-k}$ eines Abramson-Code mit gekürzten Wortlängen als Parameter;
$G(u) = (u^8 + u^7 + u^2 + u + 1)(u + 1)$;
a) $n = n_{\max} = 255$, b) $n = 200$, c) $n = 100$.
Es ist kein wesentlicher Einfluß durch die Verkürzung zu beobachten.

Dieser Code zeigt bei einer Verkürzung von $n = 255$ auf $n = 100$ keine gesicherte Änderung der Reduktionsfunktion.

In Bild 7 findet sich als weiteres Beispiel ein *Fire-Code*,

$$G(u) = (u^7 + u^3 + 1)(u^{11} + 1), \quad n_{\max} = 1397,$$

der verkürzt wurde auf

a) $n = 128$ Stellen,
b) $n = 64$ Stellen.

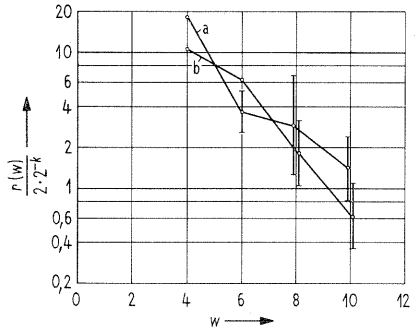


Bild 7. Durch Test ermittelte Reduktionsfunktionen $r(w)$ eines Fire-Code mit gekürzten Codewortlängen als Parameter;
$G(u) = (u^7 + u^3 + 1)(u^{11} + 1)$, $n_{\max} = 1397$;
a) $n = 128$, b) $n = 64$.

Für obigen Code ist im ungekürzten Fall als Reduktionsfaktor $r(4) = 24 \cdot 2 \cdot 2^{-k}$ zu erwarten ($k_2 = 11$ in Bild 2). Bei der Verkürzung von $n_{\max} = 1397$ auf $n = 128$ bzw. $n = 64$ verringert sich $r(4)$ nur wenig. Insgesamt zeigt auch dieser Code bei Verkürzung keine auffällige Veränderung der Reduktionsfunktion.

In etwas anderer Weise wird der Einfluß der Verkürzung in Bild 8 dargestellt. Es handelt sich um einen erweiterten *Bose-Chauduri-Code*,

$$G(u) = (u^8 + u^4 + u^3 + u^2 + 1) \times (u^8 + u^6 + u^5 + u^4 + u^2 + u + 1) \times (u + 1)$$

und $n_{\max} = 255$, dessen Hammingdistanz durch den Faktor $(u + 1)$ von $h = 5$ auf $h = 6$ erhöht wurde. (Dieses Verfahren entspricht der Erweiterung des Hamming-Code zum Abramson-Code, wodurch Fehlermuster mit ungerader Fehlerzahl sicher erkennbar werden.)

Bild 8 zeigt den Reduktionsfaktor $r(6)$ für $w = 6$ Fehlerstellen abhängig von der Codewortlänge n.

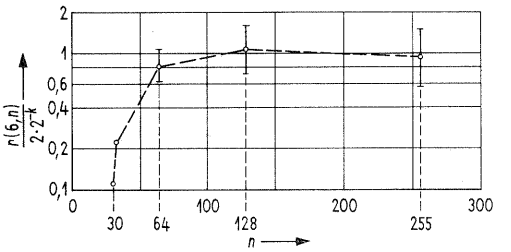


Bild 8. Durch Test ermittelter Reduktionsfaktor $r(6)$ eines erweiterten Bose-Chauduri-Code bei variabler Codewortlänge n;
$G(u) = (u^8 + u^4 + u^3 + u^2 + 1)(u^8 + u^6 + u^5 + u^4 + u^2 + u + 1)(u + 1)$,
$n_{\max} = 255$.

Man sieht, daß der Reduktionsfaktor $r(6)$ sich bei Verkürzung von $n = 255$ auf $n = 64$ nicht wesentlich ändert. Jedoch sinkt bei weiterer Verkürzung auf $n = 30$ der Reduktionsfaktor ab und wird sogar zu $r(6) = 0$ für $n < 30$. Das bedeutet, daß die Hammingdistanz dieses untersuchten Code bei Verkürzung unter $n = 30$ sich mindestens auf $h = 8$ vergrößert.

Die Verkürzung eines Code kann dessen Reduktionsfaktoren nicht nur verkleinern, sondern auch vergrößern. Im letzteren Fall bewirkt also die Verringerung der m Nachrichtenstellen je Codewort trotz gleichbleibender Anzahl der k Prüfstellen eine Verschlechterung der fehlererkennenden Eigenschaften. Beide Fälle sind in einem tabellarischen Vergleich von Code-Testergebnissen enthalten.

In der Tabelle I sind die durch Tests ermittelten Reduktionsfaktoren $r(w = 4)$ und $r(w = 6)$ bezogen auf $2 \cdot 2^{-k}$ für einige verkürzte *Abramson-* und *Fire-Codes* zusammengestellt. Die Codewortlängen wurden auf $n = 128$ bzw. $n = 64$ gekürzt. Alle Codes haben die gleiche Anzahl von $k = 18$ Prüfstellen. Die Hammingdistanzen sind im ungekürzten Fall einheitlich $h = 4$.

Tabelle I

Generatorpolynom $G(u)$	n_{max}	n_{ist}	$\frac{r(4)}{2 \cdot 2^{-k}}$	$\frac{r(6)}{2 \cdot 2^{-k}}$	$\frac{r(4)}{r_{n_{max}}(4)}$
a) Abramson-Codes					
$(u^{17} + u^3 + 1)(u + 1)$	131071	128	24,7		24,7
		64	56,5	3,7	56,5
$(u^{17} + u^3 + u^2 + u + 1)(u + 1)$	131071	128	4,32		4,32
		64	15,3	3,6	15,3
$(u^{17} + u^8 + u^4 + u^3 + 1)(u + 1)$	131071	128	0,257		0,257
		64	0	1,2	0
b) Fire-Codes					
$(u^6 + u + 1)(u^{12} + 1)$	252	128	33,8		0,83
		64	25,4	9,2	0,62
$(u^7 + u^3 + 1)(u^{11} + 1)$	1397	128	18,2		0,77
		64	10,7	6,0	0,43
$(u^7 + u^3 + u^2 + u + 1)(u^{11} + 1)$	1397	128	20,2		0,90
		64	15,8	6,5	0,70
$(u^8 + u^4 + u^3 + u^2 + 1)(u^{10} + 1)$	510	128	13,9		0,96
		64	8,25	5,1	0,57
$(u^9 + u^4 + 1)(u^9 + 1)$	5499	128	8,90		1,01
		64	77,3	4,8	8,70
$(u^9 + u^6 + u^4 + u^3 + 1)(u^9 + 1)$	5499	128	9,20		1,04
		64	0	3,4	0
$(u^{10} + u^3 + 1)(u^8 + 1)$	8184	128	2,39		0,435
		64	0	2,4	0
$(u^{13} + u^4 + u^3 + u + 1)(u^5 + 1)$	40955	128	0		0
		64	0	0,90	0
$(u^{15} + u + 1)(u^3 + 1)$	98301	128	7,0		6,7
		64	13,4	13	13,2

Innerhalb der Reduktionsfaktoren $r(4)$ läßt sich keine Systematik erkennen. Die Faktoren schwanken stark und einige verschwinden sogar, was einer Erhöhung der Hammingdistanz auf Grund der Verkürzung entspricht. Bei dem Vergleich der Reduktionsfaktoren $r(4)$ und $r(6)$ des gleichen Code und der gleichen Codewortlänge fällt auf, daß $r(6)$ stets näher an $2 \cdot 2^{-k}$ liegt als $r(4)$. Dies zeigt die Tendenz an, daß die Reduktionsfunktion $r(w)$ mit wachsendem w von unten oder von oben dem Wert $2 \cdot 2^{-k}$ zustrebt.

In der letzten Spalte der Tabelle I wurden die Reduktionsfaktoren $r(4)$ der Codewortlänge n auf $r_{n_{max}}(4)$ bezogen. Es ist $r_{n_{max}}(4)$ der Reduktionsfaktor für $w = 4$ des ungekürzten Code. Der derart bezogene Reduktionsfaktor gibt den Einfluß der Verkürzung an. Es zeigt sich, daß der bezogene Reduktionsfaktor in der letzten Spalte für $n = 128$ stets näher an 1 liegt als für $n = 64$. Mit abnehmender Verkürzung nähert sich der Reduktionsfaktor jenem des ungekürzten Code.

Alle Code-Tests zeigen demnach, daß eine geringe Verkürzung ($n_{max} > n \gg k$) die Reduktionsfunktion nur unwesentlich beeinflußt. Bei starker Verkürzung können starke Abweichungen nach jeder Richtung auftreten. Diese Abweichungen dürften aus dem Generatorpolynom direkt kaum berechenbar sein. Die Ermittlung der Reduktionsfunktion $r(w)$ bei kleinen Werten w ist für verkürzte Codes nur durch Code-Tests mit vertretbarem Aufwand möglich.

An den Ergebnissen dieser Arbeit haben Anteil Herr F. Oehme, der in einer Studienarbeit ein Rechner-Testprogramm zur Ermittlung der Reduktionsfunktion entwickelt und ausgewertet hat, sowie die Herren P. Hohm und R. Retzlaff, die in ihren Diplomarbeiten den praktischen Bau eines Code-Spezialrechners übernahmen.

Anhang 1 (zu Abschnitt 3, Gl. (15))

Bei dem Nachweis, in welchem Bereich der Stellenfehlerwahrscheinlichkeit p_E die Restfehlerwahrscheinlichkeit p_R den Wert $p_R \approx 2^{-k}$ annimmt, geht man zweckmäßig von der Betrachtung des Quersummen-Prüfschemas eines Code aus.

Das Prüfschema besteht aus k Prüfgleichungen. Würde jede der k Prüfgleichungen unabhängig von den übrigen $k - 1$ Prüfgleichungen mit der Wahrscheinlichkeit 1/2 die Fälschung des Codewortes anzeigen bzw. nicht anzeigen, so zeigen alle k Gleichungen die Fälschung nicht an mit der Wahrscheinlichkeit $(1/2)^k$. Dann ist 2^{-k} die Restfehlerwahrscheinlichkeit für gefälschte Codewörter.

Jedoch ist zu beachten, daß die Wahrscheinlichkeiten nur für statistisch unabhängige Ereignisse multipliziert werden dürfen. Da sich aber eine gefälschte Codewortstelle im allgemeinen auf mehrere Prüfgleichungen auswirkt, läßt sich diese Unabhängigkeit nur bei geeigneter Definition dieser Ereignisse erreichen. Aus diesem Grund werden die

n Codewortstellen möglichst gleichmäßig in k Klassen eingeteilt, wobei je eine Klasse nur einer Prüfgleichung zugeordnet ist. Die Aufteilung ist beliebig, mit der einen Einschränkung, daß jede Codewortstelle einer Klasse von der zugeteilten Prüfgleichung erfaßt wird. Damit sind jeder Prüfgleichung im Mittel n/k Codewortstellen als „eigene" Fehlerursachen zugeteilt.

Von den n/k Codewortstellen einer Klasse wird im stochastischen Störkanal jede Stelle unabhängig gefälscht mit der Wahrscheinlichkeit p_E. In den $n/k = n_k$ Stellen (als ganzzahlig angenommen) treten genau y Fehler auf mit der Wahrscheinlichkeit

$$p(y) = \binom{n_k}{y} p_E^y (1 - p_E)^{n_k - y}, \quad y = 0, 1, \ldots, n_k. \quad \text{(A1)}$$

Die Fälle mit ungerader Fehlerzahl y sind stets erkennbar, jene mit gerader Fehlerzahl dagegen nicht. Damit ist die Wahrscheinlichkeit für sicher erkennbare Fälle

$$\bar{p} = \sum_{y=1+2i} p(y) = \bar{p}(p_E, n_k), \quad i = 0, 1, 2, \ldots. \quad \text{(A2)}$$

Für eine Restfehlerwahrscheinlichkeit von $p_R \approx 2^{-k}$ müßte obiger Annahme entsprechend jede der k Prüfgleichungen mit der Wahrscheinlichkeit 1/2 einen Fehler innerhalb der Klasse anzeigen bzw. mit der Wahrscheinlichkeit 1/2 nicht anzeigen. Damit gilt die Restfehlerwahrscheinlichkeit $p_R \approx 2^{-k}$ mindestens für jenen Bereich von p_E, für den $\bar{p}(p_E, n_k) = 1/2$ hinreichend genau erfüllt ist.

Die Funktion $\bar{p}(p_E, n_k)$ ist in Bild A1 dargestellt. (Es ist hier von der Annäherung der Binomialverteilung Gl. (A1) durch die einfachere Poissonverteilung

$$\binom{n_k}{y} p_E^y (1 - p_E)^{n_k - y} \approx \frac{(n_k p_E)^y}{y!} e^{-n_k p_E}$$

für kleine Werte von p_E Gebrauch gemacht, weil $p_E \ll 1/2$ vorausgesetzt wird.)

Die Funktion $\bar{p}(p_E, n_k)$ weicht für Abszissenwerte $p_E n_k \geqq 2$ sehr wenig von 1/2 ab. Die relative Abweichung $(0{,}5 - \bar{p})/0{,}5$ vom Wert 1/2 ist dort kleiner als 0,018.

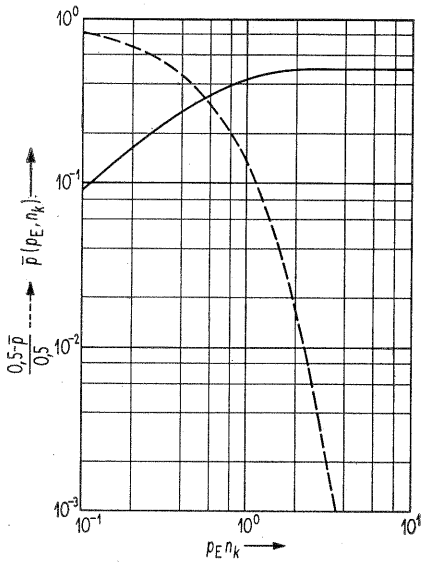


Bild A1. Es gibt $\bar{p}(p_E, n_k)$ die Wahrscheinlichkeit dafür an, daß in den $n_k = n/k$ Stellen einer Prüfgleichung ungeradzahlig viele Fehler auftreten. Mit der Wahrscheinlichkeit p_E wird dabei eine Stelle gefälscht. Für den Bereich, in dem $\bar{p} = 0{,}5$ ist, zeigt diese Prüfgleichung den Fehler an bzw. nicht an, je mit der Wahrscheinlichkeit 1/2.

Damit ist bewiesen

$$p_R \approx 2^{-k} \quad \text{für} \quad p_E \geqq 2/n_k = 2k/n. \quad \text{(A3a)}$$

Aus Gründen der Symmetrie einer Binomialverteilung bezüglich $p_E = 1/2$ folgt außerdem als Grenze für p_E nach oben

$$p_E \leqq 1 - (2k/n). \quad \text{(A3b)}$$

Anhang 2 (zu Abschnitt 4.2.4, Gl. (27))

Die Anzahl der nicht als falsch erkennbaren Muster mit vier Fehlern läßt sich aus dem Prüfschema des Fire-Code (Abschnitt 2.3.3) ablesen. Die k_2-Prüfgleichungen zeigen vier Fehler nicht an, wenn die vier Fehler in solchen Stellen liegen, die alle von nur einer der k_2 Prüfgleichungen erfaßt werden (F_1 Möglichkeiten), — oder, wenn je zwei Fehler in Stellen liegen, die paarweise von einer verschiedenen der k_2 Prüfgleichungen erfaßt werden (F_2 Möglichkeiten):

$$F(4) = F_1 + F_2. \quad \text{(A4)}$$

Für die F_1 Möglichkeiten kommen $2^{k_1} - 1 = s_1$ Fehlerstellen in Betracht (eine k_2-Gleichung festgehalten). Die Teilprüfspalten mit den k_1 Elementen dieser Stellen sind alle verschieden. Die erste Fehlerstelle kann in s_1 Stellen liegen, die zweite Fehlerstelle kann in allen restlichen $s_1 - 1$ Stellen liegen. Für die dritte Fehlerstelle gibt es jedoch nur $s_1 - 3$ Möglichkeiten: Die Summe der ersten beiden k_1-Teilprüfspalten ist gleich einer anderen Teilprüfspalte. Diese Stelle darf nicht als Ort eines Fehlers gewählt werden, da die Summe der drei k_1-Prüfspalten eine Null-Spalte ergäbe, und mit Hinzunahme des vierten Fehlers dieses Muster sicher erkennbar wäre. Als vierte Fehlerstelle ist zwangsläufig jene Stelle zu wählen, deren k_1-Prüfspalte gleich der Summe der ersten drei ausgewählten k_1-Prüfspalten ist. Damit ergibt sich

$$F_1 = k_2 \frac{s_1(s_1 - 1)(s_1 - 3)}{4!}. \quad \text{(A5)}$$

Der Nenner 4! berücksichtigt, daß die Reihenfolge der vier Fehler nicht entscheidend ist. Der Faktor k_2 berücksichtigt die Auswahl aus den k_2 Prüfzeilen.

Für die F_2 Möglichkeiten von den zweimal zwei Fehlerstellen, die je von einer der k_2 Prüfgleichungen erfaßt werden, ergibt sich

$$F_2 = \binom{k_2}{2} \binom{s_1}{2} \frac{s_1 - 1}{2!}. \quad \text{(A6)}$$

Es steht $\binom{k_2}{2}$ für die Auswahl von zwei aus den k_2 Prüfgleichungen. Innerhalb jeder k_2-Prüfgleichung kommen s_1 Fehlerpositionen in Betracht. Zwei Fehler in s_1 Stellen führen auf $\binom{s_1}{2}$ Möglichkeiten. Der dritte Fehler hat wegen der Summenspalte (mit den k_1 Elementen) nur $s_1 - 1$ Möglichkeiten, und die vierte Fehlerstelle ergibt sich wieder zwangsläufig. Mittels $2^{k_1} - 1 = s_1$ können Gl. (A4), (A5), (A6) umgeformt werden in Gl. (27).

Anhang 3 (zu Abschnitt 4.3, Gl. (29))

Als Näherung wird die im Abschnitt 3 berechnete Restfehlerwahrscheinlichkeit p_R im Bereich $2k/n \leqq p_E \leqq 1 - (2k/n)$ exakt konstant $p_R = 2^{-k}$ angenommen. Damit folgt mit Gl. (1) und Gl. (2)

$$p_R = \sum_{w=0}^{n} r(w)\, p(w) = \\ = 2^{-k} = \sum_{w=0}^{n} r(w) \binom{n}{w} p_E^w (1 - p_E)^{n-w} \quad \text{(A7)}$$

für $2k/n \leqq p_E \leqq 1 - (2k/n)$.

Ordnet man in Gl. (A7) die Summe nach Potenzen von p_E, so ergibt sich aus Gl. (A7) in ausgeschriebener Form

$$\begin{aligned}2^{-k} = {} & 1 \cdot [r(0)] + \\ & + p_E \binom{n}{1} [-r(0) + r(1)] + \\ & + p_E^2 \binom{n}{2} \left[r(0) - \binom{2}{1} r(1) + r(2)\right] + \\ & \cdots \\ & + p_E^i \binom{n}{i} \left[r(0) - \binom{i}{1} r(1) + \binom{i}{2} r(2) - \cdots - \right. \\ & \qquad \left. - \binom{i}{i-1} r(i-1) + r(i)\right] (-1)^i + \qquad \text{(A8)} \\ & \cdots \\ & + p_E^n \binom{n}{n} \left[r(0) - \binom{n}{1} r(1) + \binom{n}{2} r(2) - \cdots - \right. \\ & \qquad \left. - \binom{n}{n-1} r(n-1) + r(n)\right] (-1)^n .\end{aligned}$$

Die rechte Seite der Gl. (A8) ist ein Polynom in p_E, das aber nach Gl. (A7) innerhalb des Bereiches

$$2k/n \leqq p_E \leqq 1 - (2k/n)$$

den festen Wert 2^{-k} annimmt. Diese Unabhängigkeit von p_E für das Polynom ist nur erfüllbar, wenn alle Koeffizienten der Potenzen $p_E^1, p_E^2, \ldots, p_E^n$ verschwinden:

$$\begin{aligned} & r(0) - r(1) = 0 \\ & r(0) - \binom{2}{1} r(1) + r(2) = 0 \\ & \cdots \\ & r(0) - \binom{i}{1} r(1) + \cdots + (-1)^{i-1} \binom{i}{i-1} r(i-1) + \\ & \quad + (-1)^i r(i) = 0 \qquad \text{(A9)} \\ & \cdots \\ & r(0) - \binom{n}{1} r(1) + \cdots + (-1)^{n-1} \binom{n}{n-1} r(n-1) + \\ & \quad + (-1)^n r(n) = 0 . \end{aligned}$$

Damit folgt aus Gl. (A8)

$$r(0) = 2^{-k} .$$

Durch schrittweises Einsetzen berechnet sich mittels Gl. (A9)

$$r(0) = r(1) = r(2) = \cdots = r(n-1) = r(n) . \qquad \text{(A10)}$$

Dieses Ergebnis von Gl. (A10) muß wegen der anfänglichen Näherung, daß p_R in einem Bereich von p_E exakt konstant ist, in seinem Gültigkeitsbereich eingeschränkt werden. In Gl. (A7) werden nur Binomialverteilungen

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

benutzt mit Werten von p_E aus dem Bereich

$$2k/n \leqq p_E \leqq 1 - (2k/n) .$$

Für einen Wert von w ober- oder unterhalb der Streuung σ aller betrachteten Verteilungen $p(w)$, also außerhalb des Bereiches $2k - \sigma \leqq w \leqq n - 2k + \sigma$, ist $p(w)$ nur verschwindend klein:

$$\begin{aligned} p(w) \approx 0 \quad \text{für} \quad & w < 2k - \sigma = w_u \\ & w > n - 2k + \sigma = w_o \qquad \text{(A11)} \end{aligned}$$

wobei $\sigma^2 = 2k(1 - 2k/n)$.

Wegen Gl. (A11) beeinflußt $r(w)$ für Werte von w außerhalb des Bereiches $w_u \leqq w \leqq w_o$ die Restfehlerwahrscheinlichkeit p_R praktisch nicht. Weil aber p_R im Bereich $2k/n \leqq p_E \leqq 1 - (2k/n)$ nur näherungsweise konstant ist, darf aus Gl. (A10) keine Aussage über $r(w)$ außerhalb des Bereiches $w_u \leqq w \leqq w_o$ abgeleitet werden. Damit folgt für $r(w)$

$$r(w) = 2^{-k} \quad \text{für} \quad w_u \leqq w \leqq w_o . \qquad \text{(A12)}$$

Statt der Grenzen w_u und w_o darf man auch zur Vereinfachung die etwas engeren Grenzen $2k \leqq w \leqq n - 2k$ für den Gültigkeitsbereich von Gl. (A12) nehmen.

Schrifttum

[1] MARKO, H., Systemtechnik der Datenübertragung auf Fernsprechleitungen. Nachrichtentech. Fachber. **19** [1960], 63–69.

[2] MARKO, H. und LANGE, H., Datenübertragung und automatische Fehlerkorrektur. Jahrbuch des elektrischen Fernmeldewesens, Band 14, Bad Windsheim 1963, S. 122–164.

[3] AULHORN, H., LANGE, H. und MARKO, H., Probleme und Anwendungen der Datenübertragung. Elektron. Rechenanl. **3** [1961], 148–159.

[4] BERGER, E. R., Die Wirksamkeit von Blocksicherungsverfahren gegenüber gebündelten Störungen bei der Datenübertragung. A.E.Ü. **16** [1962], 51–55.

[5] BERGER, E. R., Codierung und Fehlersicherheit in informationstheoretischer Sicht. Nachrichtentech. Z. **11** [1963], 87–91.

[6] PETERSON, W. W. und BROWN, D. T., Cyclic codes for error detection. Proc. Inst. Radio Engrs. **49** [1961], 228–235.

[7] MEGGITT, J. E., Error correcting codes and their implementation for data transmission systems. Transact. Inst. Radio Engrs. IT-**7** [1961], 234–244.

[8] PETERSON, W. W., Error-correcting codes. J. Wiley & Sons, Inc., New York 1962.

[9] ELSPAS, B., The theory of autonomous linear sequential networks. Transact. Inst. Radio Engrs. CT-**6** [1959], 45–60.

[10] ABRAMSON, M. M., A class of systematic codes for non-independent errors. Transact. Inst. Radio Engrs. IT-**5** [1959], 150–157.

[11] BOSE, R. C. und CHAUDURI, D. K., A class of error correcting binary group codes. Information and Control **3** [1960], 68–79.

[12] HAMMING, R. W., Error detecting and error correcting codes. Bell Syst. tech. J. **29** [1950], 147–160.

[13] FIRE, P., A class of multiple-error-correcting binary codes for non-independent errors. Sylvania Report RSL-E-2, 1959, Sylvania Laboratory Mountain View, Calif.

[14] ELLIOTT, E. O., Estimates of error rates for codes on burst-noise channels. Bell Syst. tech. J. **42** [1963], 1977–1997.

[15] MCWILLIAMS, J., A theorem on the distribution of weights in a systematic code. Bell Syst. tech. J. **42** [1963], 79–94.

[16] SLEPIAN, D., Some further theory of group codes. Bell Syst. tech. J. **39** [1960], 1219–1252.

[17] NILI, H., Fehlerwahrscheinlichkeit und Geschwindigkeit bei Übertragung digitaler Informationen durch Gruppen-Codes. A.E.Ü. **18** [1964], 282–292.

[18] NILI, H., Matrixschaltungen zur Codierung und Decodierung von Gruppen-Codes. A.E.Ü. **18** [1964], 555–564.