Reed-Solomon-Codes zur Mehrblock-Bündelfehler-Korrektur

Wie die zyklischen **BCH-Codes** zur Mehrbitfehler-Korrektur eignen sich auch die sehr verwandten **Reed-Solomon-Codes** (= RS-Codes) zur Mehrbitfehler-Korrektur. Die Konstruktion der Codewort-Polynome und das Korrekturverfahren sind beinahe identisch. Die Unterschiede bestehen in folgenden beiden Besonderheiten:

- Die unabhängige Polynomvariable x und die Koeffizienten der beteiligten Polynome sind Elemente des Galoisfeldes $GF(2^{m^*})$, welches durch die Nullstelle des **definierenden irreduziblen Polynoms**

  $$g^*(x)=g^*_{m^*}\cdot x^{m^*} + g^*_{m^*-1}\cdot x^{m^*-1} + ... + g^*_1\cdot x^1 + g^*_0$$

  gegeben ist. Für $m^* = 3$ und $g^*(x)=1011$ hatten wir die Nullstelle mit α bezeichnet, für $m^* = 4$ und $g^*(x)=10011$ mit β und so weiter.

  Die Elemente können durch ihre binäre Kurzform dargestellt werden und haben dann die Bitbreite m^*. In einem Galoisfeld GF(2^3) etwa entspricht dem Element α^6 die binäre Kurzform 101. Damit ist die Verbindung zwischen der abstrakten Rechen- und der realen technischen Welt gegeben.

- Das Generatorpolynom ist für t_{korr} korrigierbare Fehlerbündel der binären Bitbreite m^* das Produkt aus $2\cdot t_{korr}$ Linearfaktoren

  $$g(x)=\prod_{i=1}^{i=2\cdot t_{korr}} \left(x - \alpha^i\right) .$$

  Die Galoisfeld-Elemente α stehen hier stellvertretend für Galoisfeld-Elemente der Ordnung 2^{m^*} . Für das Galoisfeld $GF(2^3)$ und $t_{korr}=1$ Fehlerbündel der Bitbreite 3 ergibt sich das Generatorpolynom

  $$g(x)=\prod_{i=1}^{i=2} \left(x - \alpha^i\right)=(x-\alpha^1)\cdot(x-\alpha^2) ,$$

  für $t_{korr}=2$ entsprechend

  $$g(x)=\prod_{i=1}^{i=4} \left(x - \alpha^i\right)=(x-\alpha^1)\cdot(x-\alpha^2)\cdot(x-\alpha^3)\cdot(x-\alpha^4) .$$

Alle weiteren Aussagen bleiben formal die Gleichen wie beim BCH-Code. Die Koeffizienten wie u_1, u_2, … y_1, y_2, ... haben in binärer Kurzform jedoch die Bitbreite m^* .

Codewortdarstellung als n-Tupel von Info- und Prüf-Elementen der binären Blockbreite m^* :

$$v=\left(u_1\ u_2\ ...\ u_k\ y_1\ y_2\ ...y_m\right) = \left(v_1\ v_2\ ...\ v_n\right) , n=m+k$$

Die Positionen der Info- und Prüfbits sind durch die geordnete Struktur und die Indices eindeutig festgelegt. In binärer Kurzform hat eine Codewort nun die **Bitlänge** $n_b=n\cdot m^*$.

Beispiele:

- Im $GF(2^3)$ kann ein Codewort als Anordnung von

  $n=2^3-1=7$ Elementen des Galoisfeldes

  oder als Anordnung von

  $n_b=(2^3-1)\cdot 3=21$ Bits in 7 Binärblöcken dargestellt werden.

- Im $GF(2^4)$ sind es $n=2^4-1=15$ Elemente oder $n_b=(2^4-1)\cdot 4=60$ Bits.

Codewortdarstellung alternativ als Polynom mit Koeffizienten über $GF(2^{m^*})$:

$$v=v(x)=u_1\cdot x^{n-1} + u_2\cdot x^{n-2} + ...+ u_k\cdot x^{n-k+1} + y_1\cdot x^{n-k-2} + y_2\cdot x^{n-k-3} +...+ y_{m-1}\cdot x^1+y_m$$

Die Positionen der Info- und Prüf-Elemente mit der binären Blockbreite m^* sind durch die Zuordnung als Koeffizienten der x-Potenzen eindeutig festgelegt.

Weitere Definitionen:

Info-Polynom: $$u(x)=u_1\cdot x^{k-1} + u_2\cdot x^{k-2} + ...+ u_{k-1}\cdot x^1 + u_k \qquad (I)$$

Die k Koeffizienten können jedes beliebige Binärmuster der Blockbreite m^* annehmen. **Zum Beispiel** bilden im $GF(2^3)$ die 15 Infobits

u = 101 111 000 010 001

das Infopolynom $u(x)=\alpha^6\cdot x^4 + \alpha^5\cdot x^3 + 0\cdot x^2 + \alpha^1\cdot x^1 + \alpha^0$ oder in Kurzform

$$u(x)=\alpha^6\ \ \alpha^5\ \ 0\ \ \alpha^1\ \ \alpha^0$$

Prüfpolynom: $$y(x)=y_1\cdot x^{m-1} + u_2\cdot x^{m-2} + ...+ y_{m-1}\cdot x^1 + y_m \qquad (II)$$

Die m Koeffizienten können jede beliebige Elementanordnung des zugrunde gelegten Galoisfeldes annehmen. Diese stellt eine Funktion der k Info-Blöcke dar.

Stellenweise Addition und Subtraktion von Polynomen: Wie bei den BCH-Codes werden auch hier Polynome addiert (subtrahiert), indem man die Koeffizienten **gleicher** x-Potenzen addiert (subtrahiert).

Bildungsvorschrift für RS-Codewortpolynome (wie bei BCH-Codes):

$$v(x)=u(x)\cdot x^m \;+\; \left[u(x)\cdot x^m\right] \;\text{MOD}\; g(x)$$

Im ersten Term auf der rechten Seite wird das Info-Polynom u(x) durch Multiplikation mit x^m um m Positionen nach links geschoben und erhält nach den Rechenregeln für Polynome den Grad

$$\text{grad}\left[u(x)\cdot x^m\right]=k-1+m \quad .$$

Die rechts nachrückenden Potenzen x^{m-1} bis x^0 (=1) haben alle die Koeffizienten „0“. An diesen Stellen wird „Platz“ geschaffen für die Koeffizienten des Ergebnisses aus dem zweiten Term. Die Modulo-Operation MOD ist hier der Rest des Polynomdivision $u(x)\cdot x^m$ durch das Generatorpolynom und ergibt das gesuchte Prüfpolynom y(x)

$$y(x)=r(x)=\left[u(x)\cdot x^m\right] \;\text{MOD}\; g(x) \quad . \qquad \text{(VIII)}$$

Wegen der stellenweisen Addition von Polynomkoeffizienten baut sich das Codewortpolynom als systematische Struktur aus dem Info-Polynom und dem Prüfpolynom auf, in Kurzform

$$v(x)=u_1\;\; u_2\;\; \ldots\;\; u_k\;\; y_1\;\; y_2\;\; \ldots + y_m \quad .$$

Grad des Prüfpolynoms y(x) bzw. des Restpolynoms r(x): Nach den Regeln der Modulo-Operation hat das Ergebnis stets höchstens den Grad des Generatorpolynoms minus 1:

$$\text{grad}\left[y(x)\right] \;\le\; \text{grad}\left[g(x)\right]-1 \;=\; m-1 \;=\; 2\cdot t_{korr}-1 \quad .$$

Das Prüfpolynom weist also höchstens $m=2\cdot t_{korr}$ von Null verschiedene Koeffizienten auf und „passt“ daher bei Addition immer unverändert in den rechts liegenden Teil des um x^m nach links verschobenen Info-Polynoms

$$u(x)\cdot x^m \quad .$$

Haupteigenschaft des Codewortpolynoms v(x):

v(x) ist ein **Vielfaches** des Generatorpolynoms g(x), d h. der Divisionsrest ist Null (ohne Nachweis):

$$v(x) \;\text{MOD}\; g(x) \;=\; 0$$

Hat man also ein Empfangswort w(x) erhalten, welches fehlerfrei aus v(x) entstand, so ergibt sich bei der MOD-Division das Nullpolynom (Nullpolynom = alle Koeffizienten sind 0).

Alternativ und für den praktischen Gebrauch besser geeignet ist die Eigenschaft, dass jedes Codewort-Polynom für die Nullstellen des Generator-Polynoms immer den Wert 0 annimmt.

Beispiel für $GF(2^3)$ und $t_{korr}=2$:

$$v(x=\alpha^1)=0$$

$$v(x=\alpha^2)=0$$

$$v(x=\alpha^3)=0$$

$$v(x=\alpha^4)=0 \quad .$$

Fehlerpolynom e(x): Wenn der Code für t_{korr} korrigierbare Fehlerblöcke der binären Breite m^* aufgebaut wurde, dürfen im Empfangswort-Polynom höchstens t_{korr} Fehlerblöcke enthalten sein. Diese kann man für die theoretische Betrachtung in einem Polynom höchstens des Grades n-1 erfassen, bei dem höchstens t_{korr} Koeffizienten den Wert e_i , $i \in 0,\ 1,\ 2,\ ....\ ,\ n-1$, aufweisen. Dabei ist e_i ein Element des zugrunde liegenden Galoisfeldes oder in binärer Form ein Binärblock der Breite $b=m^*$.

Beispiel für $GF(2^3)$ und $t_{korr}=2$: Sind an den Positionen 5 (bei x^5) und 2 (bei x^2) die Fehlerwerte

$$e_5=101 \rightarrow \alpha^6 \quad \text{und} \quad e_2=011 \rightarrow \alpha^3$$

aufgetreten, so hat das Fehlerpolynom – welches man allerdings vor der Korrektur nicht kennt – die Form

$$e(x)=\alpha^6 \cdot x^5+\alpha^3 \cdot x^2 \quad \text{oder in binärer Kurzschreibweise}$$

$$e(x)=000\ \ 101\ \ 000\ \ 000\ \ 011\ \ 000\ \ 000 \quad .$$

Anders als beim Fehlerpolynom des BCH-Codes ist hier jeder Fehlerblock eindeutig durch die **Fehlerposition** und den **Fehlerwert** gekennzeichnet. Die Aufgabe bei der Fehlerkorrektur besteht beim RS-Code also darin

- die Fehlerposition
- und den Fehlerwert

zu bestimmen.

Das Empfangswort-Polynom w(x) stellt wieder die Summe aus dem Codewort-Polynom und dem Fehlerpolynom dar:

$$w(x)=v(x)+e(x) \quad .$$

Syndrompolynom s(x): Verbleibt bei der Division des Empfangswortpolynoms w(x)

$$w(x)\ \text{MOD}\ g(x) = s(x) \neq \text{Nullpolynom}$$

ein vom Nullpolynom verschiedenes Restpolynom, so nennt man es Syndrompolynom s(x), da es auf ein „krankes“, d. h. fehlerbehaftetes Polynom w(x) verweist. Aus dem Wert des Syndrompolynoms lässt sich auf die Fehlerpositionen schließen.

Auch hier sind die Nullstellen des Generator-Polynoms besser für den Gebrauch geeignet:

$$s(x=\alpha^1)=w(x=\alpha^1)=v(\alpha^1)+e(\alpha^1)=0+e(\alpha^1)=e(\alpha^1)$$

$$s(x=\alpha^2)=w(x=\alpha^2)=v(\alpha^2)+e(\alpha^2)=0+e(\alpha^2)=e(\alpha^2)$$

$$s(x=\alpha^3)=w(x=\alpha^3)=v(\alpha^3)+e(\alpha^3)=0+e(\alpha^3)=e(\alpha^3)$$

usw. Der Wert der Syndrompolynome hängt also nur vom Fehler-Polynom und nicht vom Codewort-Polynom ab.

Beispiel für $GF(2^3)$ und $t_{korr}=2$:

Die – noch – unbekannten Fehler-Blöcke lassen sich allgemein im Fehler-Polynom

$$e(x)=e_i\cdot x^i+e_j\cdot x^j$$

darstellen, wobei sowohl die Positions-Exponenten i und j , als auch die Fehlerwerte e_i und e_j unbekannt sind. Die 4 Syndrome ergeben sich daraus als die 4 Werte

$$s(\alpha^1)=e(\alpha^1)=e_i\cdot(\alpha^1)^i+e_j\cdot(\alpha^1)^j = e_i\cdot\alpha^i+e_j\cdot\alpha^j$$

$$s(\alpha^2)=e(\alpha^2)=e_i\cdot(\alpha^2)^i+e_j\cdot(\alpha^2)^j = e_i\cdot\alpha^{2\cdot i}+e_j\cdot\alpha^{2\cdot j}$$

$$s(\alpha^3)=e(\alpha^3)=e_i\cdot(\alpha^3)^i+e_j\cdot(\alpha^3)^j = e_i\cdot\alpha^{3\cdot i}+e_j\cdot\alpha^{3\cdot j}$$

$$s(\alpha^4)=e(\alpha^4)=e_i\cdot(\alpha^4)^i+e_j\cdot(\alpha^4)^j = e_i\cdot\alpha^{4\cdot i}+e_j\cdot\alpha^{4\cdot j}$$

Für die 4 Unbekannten stehen also 4 Gleichungen zur Verfügung, eine notwendige Voraussetzung für die Lösung.

Aufgabe: Bestimmen Sie für den Informationsbit-Strom 000 000 000 011 111 … das RS-Codewort v(x) für $t_{korr}=1$ unter Zugrundelegung des $GF(2^3)$.

Hilfsfragen:

- Welchen Grad hat g*(x)?
- Welche Länge n hat ein Codewort?
- Was ist das Generatorpolynom g(x)
- Wie viele Infostellen k hat ein Codewort in der Form mit Galoisfeld-Elementen und als binäre Blöcke?