Zyklische Codes in Polynomdarstellung mit Koeffizienten über Z_2 für Mehrbitfehler-Korrektur

Codewortdarstellung als n-Tupel von Info- und Prüfbits:

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

Die Positionen der Info- und Prüfbits sind durch die geordnete Struktur und die Indices eindeutig festgelegt.

Codewortdarstellung als Polynom mit Koeffizienten über Z_2 :

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

Die Position der Info- und Prüfbits ist durch die Zuordnung als Koeffizienten der x-Potenzen eindeutig festgelegt. Abgesehen vom höheren Schreibaufwand unterscheiden sich die beiden Darstellungen inhaltlich bezüglich der Info- und Prüfbits aber nicht. Der Vorteil besteht darin, dass Codewörter nun mit den Rechenregeln für Polynome gebildet und verarbeitet werden können und dadurch weitere Leistungen verfügbar sind, als bei der Tupel-Darstellung. Insbesondere lassen sich hiermit Verfahren zur Mehrbitfehler-Korrektur aufbauen.

Weitere Definitionen:

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

Die k Koeffizienten können jede beliebige Binäranordnung annehmen, die dem zu codierenden Informationsblock entspricht.

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

Die m Koeffizienten können jede beliebige Binäranordnung annehmen. Diese stellt aber eine Funktion der k Infobits dar.

Grad eines Polynoms: Der höchste mögliche Exponent bei x. Zum Beispiel hat u(x) den Grad

$$\text{grad}\,[u(x)]=k-1\ .$$
(III)

Definierendes irreduzibles Polynom g*(x) vom Grad m* mit Koeffizienten über Z_2, kurz „Polynom über Z_2“:

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

Es ist ein Polynom, dass sich **nicht** als Produkt von Polynomen kleineren Grades darstellen lässt und entspricht damit bei den Polynomen den Primzahlen in der Menge der natürlichen Zahlen. Auch hier gilt mit

$$\text{grad}\,[g^*(x)]=m^*\ \text{ immer }\ g^*_{m^*}=1\ \text{ und }\ g^*_0=1\ \text{ (Grund ?)}$$

Es gibt zu jedem Grad $m^* \in N,\ m^* = 1,\ 2,\ 3,\ ....$ mindestens ein irreduzibles Polynom, meist aber mehrere. Bei Polynomen über Z_2 zum Beispiel:

m*=1: $x+1$

m*=2: x^2+x+1

m*=3: x^3+x+1 , x^3+x^2+1

m*=4: x^4+x+1 , $x^4+x^3+x^2+x+1$, x^4+x^3+1

m*=5: x^5+x^2+1 , $x^5+x^4+x^3+x^2+1$, $x^5+x^4+x^2+x+1$ und 3 Weitere.

Mit dem Grad wächst auch die Anzahl (aber nicht proportional), man kann die Polynome leicht selbst bestimmen oder in Tabellen nachsehen.

Länge n des Codewortes und Grad m* des irreduziblen Polynoms: Die Stellenzahl oder Länge n des Codewort-Polynoms berechnet sich (hier ohne Nachweis) aus:

$$n = 2^{m^*} - 1 \qquad \text{(V)}$$

Kurzdarstellung von Polynomen: Wenn man die Eigenschaft der x-Potenzen als Positions-Festlegung der zugehörigen Koeffizienten ansieht, kann man jedes Polynom als n-Tupel der Koeffizienten darstellen und so die Schreibarbeit verringern und die Übersichtlichkeit erhöhen. Zum Beispiel ist in Kurzform

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

Das irreduzible Polynom vom Grad m*=2:

$$g^*(x) = 1\,1\,1\ .$$

Das definierende irreduzible Polynom vom Grad m*=3:

$$g^*(x) = 1\,0\,1\,1 \quad \text{usw.}$$

Stellenweise Addition und Subtraktion von Polynomen: Nach den Rechenregeln für Polynome werden Polynome addiert (subtrahiert), indem man die Koeffizienten **gleicher** x-Potenzen addiert (subtrahiert).

Generatorpolynom: $g(x) = g_m \cdot x^m + g_{m-2} \cdot x^{m-1} + ... + g_1 \cdot x^1 + g_0$ (VI)

Das Generatorpolynom „generiert“ (= erzeugt) die Codewörter und bestimmt die Eigenschaften für die Fehlerkorrektur.

Generatorpolynome sind für

- 1-Bitfehler-korrigierende Codes **immer** irreduzible Polynome vom Grad m=m*
- für t-Bitfehler-korrigierende Codes **immer Produkte** aus t irreduziblen Polynomen.

Bestandteil jedes Generatorpolynoms g(x) ist das definierende irreduzible Polynom $g^*(x)$ des gewählten Grades.

Für die Koeffizienten gilt dann das gleiche wie für die irreduziblen Polynome, aus denen sie sich aufbauen:

$$g_m = 1 \quad \text{und} \quad g_0 = 1 \quad .$$

Mit diesen Definitionen kann nun die Bildungsvorschrift für Codewortpolynome aufgebaut werden:

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

Im ersten Term auf der rechten Seite wird das Info-Polynom u(x) durch Multiplikation mit x^m um Stellen 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 der 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:

$$\text{grad}\left[y(x)\right] \; \leq \; \text{grad}\left[g(x)\right] - 1 \; = \; m - 1 \quad .$$

Das Prüfpolynom weist also höchstens „m“ von Null verschiedene Koeffizienten auf und „passt“ daher bei Addition gemäß (VI) 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) ist ein **Vielfaches** des Generatorpolynoms g(x), d h. der Divisionsrest ist Null (ohne Nachweis):

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

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).

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

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

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.

Fehlerpolynom e(x): Wenn der Code für t_{korr} korrigierbare Fehler aufgebaut wurde, dürfen im Empfangswort-Polynom höchstens t_{korr} Fehler 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 1 aufweisen. Das Empfangswort e(x) stellt dann die Summe aus dem Codewort-Polynom und dem Fehlerpolynom dar:

$$w(x) = v(x) + e(x) = v(x) + \left(x^i + x^j + \ldots\right) \quad \text{(immer MOD 2).} \qquad \text{(XI)}$$

Die i, j, … sind die Fehlerpositionen. Jeder „1“-Koeffizient in e(x) „kippt“ damit das zugehörige Bit im Codewort-Polynom. Für die Decodierung hat dies allerdings keinen Nutzen, da man die Fehler ja gerade nicht kennt.

Einfluss des Fehlerpolynoms auf das Syndrompolynom: Nach den Rechenregeln der Modulo-Operationen kann die Modulo-Division einer Summe auch als Modulo-Summe der Modulo-Division der Summanden ausgeführt werden:

$$s(x) = w(x)\ \text{MOD}\ g(x) = \left[v(x) + e(x)\right]\ \text{MOD}\ g(x) \qquad \text{(XII)}$$

$$= \left[v(x)\ \text{MOD}\ g(x) + e(x)\ \text{MOD}\ g(x)\right]\ \text{MOD}\ g(x)$$

und wegen (IX)

$$s(x) = e(x)\ \text{MOD}\ g(x) \qquad \text{(XIII)}$$

Das Syndrompolynom ist also **nur** vom Fehlerpolynom, nicht aber vom Codewortpolynom abhängig.

Aufgabe: Bestimmen Sie für den Informationsbit-Strom 0000 0000 0110 0111 … das Codewort v(x) für 1-Bitfehler-Korrektur unter Zugrundelegung des definierenden irreduziblen Polynoms über Z_2

$$g^*(x) = 10011 \quad .$$

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?