Beispiel zur Decodierung eines Reed-Solomon-Empfangswortes

Um die Wirkung von Fehlern beim Decodieren eines Empfangswortes w(x) verfolgen zu können, wird ein Codewort-Polynom v(x) gewählt und mit einem Fehlerpolynom e(x) verfälscht.

Als zugrunde liegendes Galoisfeld ist hier GF(2^3) mit dem definierenden irreduziblen Polynom

$g^*(x)=1011$ und der Nullstelle α

vorgesehen. Das vollständige Galoisfeld mit allen 8 Elementen findet man im Infoblatt

„Galoisfelder_GF_2_hoch_3_und_GF_2_hoch_4.pdf“

Die Anzahl korrigierbarer Fehler-Blöcke der Breite m* = 3 soll t_{korr} = 1 sein. Dann berechnet sich das RS-Generatorpolynom gemäß dem Infoblatt

„Zyklische_Codes_2_Reed_Solomon.pdf“.

aus $g(x)=\prod_{i=1}^{i=2}(x - \alpha^i)=(x-\alpha^1)\cdot(x-\alpha^2) = x^2+\alpha^4\cdot x+\alpha^3 \rightarrow 001\ \ 110\ \ 011$.

Als Codewort-Polynom wird das aus dem Hilfsblatt zur MOD [g(x)]-Division Berechnete gewählt:

$$v(x)=0\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 0\cdot x^3 + \alpha^3\cdot x^2 + 1\cdot x^1+\alpha^6$$

$$v(x)=000\ \ 000\ \ 000\ \ 000\ \ 011\ \ 001\ \ 101 \quad .$$

Der Fehler soll an der Position bei x^4 auftreten und den Fehlerwert $e_4=101$ haben. Das Fehler-Polynom (hier nur als „Laborversuch“ ausnahmsweise **vorher** bekannt!) ist dann

$$e(x)=0\cdot x^6+0\cdot x^5+\alpha^6\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x^1+0\cdot 1 = \alpha^6\cdot x^4$$

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

Das Empfangswort-Polynom w(x) entsteht daraus synthetisch als MOD 2 -Summe:

$$w(x)=v(x)+e(x)=0\cdot x^6 + 0\cdot x^5 + \alpha^6\cdot x^4 + 0\cdot x^3 + \alpha^3\cdot x^2 + 1\cdot x^1+\alpha^6$$

$$w(x)=000\ \ 000\ \ 101\ \ 000\ \ 011\ \ 001\ \ 101 \quad .$$

Lässt man die Terme mit den 0-Koeffizienten weg, erhält man den etwas besser lesbaren Ausdruck

$$w(x)=\alpha^6\cdot x^4 + \alpha^3\cdot x^2 + 1\cdot x^1+\alpha^6$$

Hiermit werden die beiden Syndromwerte

$$s(x=\alpha^1)=w(\alpha^1)=\alpha^6\cdot(\alpha^1)^4 + \alpha^3\cdot(\alpha^1)^2 + 1\cdot(\alpha^1)^1+\alpha^6$$

$$s(x=\alpha^2)=w(\alpha^2)=\alpha^6\cdot(\alpha^2)^4 + \alpha^3\cdot(\alpha^2)^2 + 1\cdot(\alpha^2)^1+\alpha^6 \quad \text{bestimmt:}$$

$$s(x=\alpha^1)=\alpha^6\cdot\alpha^4 \;+\; \alpha^3\cdot\alpha^2 \;+\; 1\cdot\alpha^1+\alpha^6 \;=\; \alpha^{10} \;+\; \alpha^5 \;+\; \alpha^1+\; \alpha^6$$

$$s(x=\alpha^2)=\alpha^6\cdot\alpha^8 \;+\; \alpha^3\cdot\alpha^4 \;+\; 1\cdot\alpha^2+\alpha^6 \;=\; \alpha^{14} \;+\; \alpha^7 \;+\; \alpha^2 \;+\; \alpha^6$$

Die Exponenten der $\alpha-\text{Elemente}$ müssen wegen der Periodizität mit 7 noch der MOD 7-Operation unterzogen werden:

$$s(x=\alpha^1) \;=\; \alpha^{10} \;+\; \alpha^5 \;+\; \alpha^1+\; \alpha^6 \;=\; \alpha^3 \;+\; \alpha^5 \;+\; \alpha^1 \;+\; \alpha^6$$

$$s(x=\alpha^2) \;=\; \alpha^{14} \;+\; \alpha^7 \;+\; \alpha^2 \;+\; \alpha^6 \;=\; \alpha^0 \;+\; \alpha^0 \;+\; \alpha^2 \;+\; \alpha^6 \;\;.$$

Zur Addition der $\alpha-\text{Elemente}$ verwendet man am Besten die binäre Kurzform:

$$s(x=\alpha^1) \;=\alpha^3 \;+\; \alpha^5 \;+\; \alpha^1 \;+\; \alpha^6 \;\rightarrow\; 011+111+010+101 \;=\; 011 \;\rightarrow\; \alpha^3$$

$$s(x=\alpha^2) \;=\; \alpha^0 \;+\; \alpha^0 \;+\; \alpha^2 \;+\; \alpha^6 \;\rightarrow\; 000+000+100+101 \;=\; 001 \;\rightarrow\; \alpha^0 \;=\; 1 \;\;.$$

Mit dem Fehlermodell für t_{korr} = 1 (ein einziger Fehlerblock an der Stelle x^i mit dem Wert e_i)

$$w(x)=v(x)+e(x)=v(x)+e_i\cdot x^i$$

lassen sich bei Beachtung von $v(\alpha^1)=0$ und $v(\alpha^2)=0$ die Syndromwerte auch als

$$s(\alpha^1) \;=\; e_i\cdot\left(\alpha^1\right)^i \;=\; e_i\cdot\alpha^i \;=\; \alpha^3 \qquad\qquad \text{(I)}$$

$$s(\alpha^2) \;=\; e_i\cdot\left(\alpha^2\right)^i \;=\; e_i\cdot\alpha^{2i} \;=\; 1 \;\; \text{schreiben.} \qquad\qquad \text{(II)}$$

Damit liegen zwei Gleichungen zur Bestimmung der beiden Unbekannten „Position i“ und „Fehlerwert e_i“ vor. Zu ihrer Ermittlung kann man z. B. (I) nach e_i auflösen und in (II) einsetzen:

$$e_i \;=\; \frac{\alpha^3}{\alpha^i} \;\rightarrow \text{in (II)} \rightarrow\; \frac{\alpha^3}{\alpha^i}\cdot\alpha^{2i} \;=\; 1 \;\rightarrow\; \alpha^3\cdot\alpha^i \;=\; 1 \;\rightarrow\; \alpha^i \;=\; \frac{1}{\alpha^3} \;=\; \alpha^{-3} \;=\; \alpha^4$$

Dabei ist **immer** zu beachten: Wegen der Periodizität der $\alpha-\text{Elemente}$ werden die Exponenten der MOD 7 – Operation unterzogen, es gilt deshalb

$$\alpha^{-3} \;=\; \alpha^{(-3)\ \text{MOD}\ 7} \;=\; \alpha^4 \;\;.$$

Durch Vergleich der Exponenten i = 4 erhält man die Fehlerposition bei x^4. Dieses Ergebnis kann man z. B. in (I) einsetzen:

$$e_i\cdot\alpha^i \;=\; e_i\cdot\alpha^4 \;=\; \alpha^3 \;\rightarrow\; e_i \;=\; \frac{\alpha^3}{\alpha^4} \;=\; \alpha^{-1} \;=\; \alpha^{(-1)\ \text{MOD}\ 7} \;=\; \alpha^6 \;\rightarrow\; 101 \;\;.$$

Damit ist auch der Fehlerwert bekannt und man kann durch MOD 2 -Addition von $e_i=101$ zum Koeffizienten 101 bei x^4 des Empfangswort-Polynoms w(x) die Korrektur durchführen. Damit liegt der **Schätzwert** $\tilde{v}(x)$ für das Codewort-Polynom v(x) als

$$\tilde{v}(x) = 000\ 000\ 000\ 000\ 011\ 001\ 101$$ vor.

Die Bezeichnung „Schätzwert“ muss deshalb gewählt werden, weil man nicht vollkommen sicher sein darf, dass es sich um das gesendete Codewort-Polynom handelt. Es könnte mehr als ein Fehler-Block aufgetreten sein, was man aber ohne weiter Maßnahmen nicht bemerken würde. Da der RS-Code im vorliegenden Fall aber nur für die Korrektur eines Fehlerblockes aufgebaut ist, ergäbe der Korrektur-Algorithmus ein falsches Codewort-Polynom.

Aufgabe 1: Unter Zugrundelegung gleicher Voraussetzungen, also GF(2^3) und t_{korr} = 1, erhalten Sie das Empfangswort

$$w(x) = 000\ 000\ 000\ 000\ 011\ 111\ 101 \quad .$$

Bestimmen Sie den Schätzwert $\tilde{v}(x)$.

Aufgabe 2: Bestimmen Sie für die Info-Bits u = 000 011 111 000 000 das RS-Codewort-Polynom für t_{korr} = 2 Fehler-Block-Korrektur.

Aufgabe 3: Wählen Sie willkürlich zwei Fehler-Blöcke an irgendwelchen Positionen, berechnen Sie sich aus dem Codewort-Polynom von Aufgabe 2 das zugehörige Empfangswort-Polynom w(x) und prüfen Sie, ob man bei der Decodierung die vorgegebenen Fehlerblöcke erhält.