Hilfsblatt für die MOD g(x)-Division von Polynomen mit Koeffizienten über GF(2^{m^*})
- gebraucht zur Berechnung der Prüf-Polynome von Reed_Solomon-Codes -

Beispiel für einem RS-Code mit Koeffizienten über GF(2^3). Dann ist n=2^3-1=7. Die Anzahl der Bits des Codewortes beträgt n_b=(2^3-1)·3 = 21

Infobits: u = 000 000 000 000 011

Für t_{korr}=1: g(x) = $x^2 + \alpha^4 x + \alpha^3 \rightarrow$ 001 110 011

g(x) muss hier mit α^3 multipliziert werden, damit in $u(x) \cdot x^2$ bei x^2 der Koeffizient α^3 entsteht

$u(x) \cdot x^2$

x^6	x^5	x^4	x^3	x^2	x^1	X^0 =1
0 0 0	0 0 0	0 0 0	0 0 0	0 1 1	0 0 0	0 0 0
0	0	0	0	α^3	0	0
			subtrahieren →	$\alpha^3 \cdot \alpha^0 = \alpha^3$	$\alpha^7 = 1$	α^6
			„+“ = „-“ im Z_2 →	0	1=0-1	$\alpha^6 = 0-\alpha^6$
				0 0 0	0 0 1	1 0 1

→ Restpolynom

g(x)

0 0 1	1 1 0	0 1 1
α^0 =1	α^4	α^3

v(x):

x^6	x^5	x^4	x^3	x^2	x^1	X^0 =1
0 0 0	0 0 0	0 0 0	0 0 0	0 1 1	0 0 1	1 0 1
0	0	0	0	α^3	1	α^6

→ Das Restpolynom wird an das Infopolynom „angehängt“

Prüfen Sie, ob $v(x=\alpha^1) = 0$ und $v(x=\alpha^2) = 0$ ist !

Weiteres Beispiel zum Vervollständigen auf der nächsten Seite →

Andere Infobits: u = 000 000 111 000 011

Für t_{korr}=1: g(x) = $x^2 + \alpha^4 x + \alpha^3 \rightarrow$ 001 110 011

u(x) · x^2

x^6	x^5	x^4	x^3	x^2	x^1	X^0 =1
0 0 0	0 0 0	1 1 1	0 0 0	0 1 1	0 0 0	0 0 0
0	0	α^5	0	α^3	0	0
subtrahieren →		α^5	$\alpha^5\ \alpha^4 = \alpha^2$	$\alpha^5\ \alpha^3 = \alpha^1$	0	
		0	$\alpha^2 = 0 - \alpha^2$	$1 = \alpha^3 - \alpha^1$	0	
		0 0 0	1 0 0	0 0 1	0 0 0	
	subtrahieren →					
	subtrahieren →					

→ Restpolynom ?

g(x)

0	0	1	1	1	0	0	1	1
α^0 =1			α^4			α^3		

v(x):

x^6	x^5	x^4	x^3	x^2	x^1	X^0 =1
0 0 0	0 0 0	1 1 1	0 0 0	0 1 1		
0	0	α^5	0	α^3		

→ Das Restpolynom wird an das Infopolynom „angehängt“

Prüfen Sie, ob $v(x=\alpha^1) = 0$ und $v(x=\alpha^2) = 0$ ist !