Aufgabe 8 (BCH Codes)

Für einen binären Kanal soll ein 1-Fehler-korrigierender BCH-Code mit der Blocklänge $N = 31$ entworfen werden. Das Generatorpolynom $g(D)$ dieses Codes wird mit Hilfe eines erweiterten Galois-Feldes $GF(2^5)$ berechnet.

a) Welche Eigenschaft muss ein binäres Polynom $f(D)$ aufweisen, damit es zur Erzeugung eines erweiterten Galois-Feldes $GF(2^5)$ geeignet ist? Welches der folgenden Polynome könnte die geforderte Eigenschaft aufweisen? (Begründung!) Anhand welcher Beziehung könnte man das gegebenenfalls überprüfen?

$$\begin{aligned} f_1(D) &= D^4 + D + 1 \\ f_2(D) &= D^5 + D^4 + D^3 + D^2 + 1 \\ f_3(D) &= D^5 + D^4 + D^3 + 1 \end{aligned}$$

Im folgenden sei nun das erweiterte Galois-Feld $GF(2^5)$ laut Beiblatt A gegeben, das mit Hilfe des Polynoms $f(D) = D^5 + D^2 + 1$ erzeugt wurde.

b) Vervollständigen Sie die gegebene Tabelle des $GF(2^5)$ in Beiblatt A, indem Sie die 10 fehlenden Elemente in Polynomdarstellung berechnen.

c) Welcher Bedingung muss die Ordnung eines beliebigen Elementes eines erweiterten Galois-Feldes $GF(2^n)$ allgemein genügen? Welche Ordnung hat ein primitives Element eines $GF(2^n)$? Wieviele primitive Elemente eines $GF(2^5)$ gibt es insgesamt?

d) Lösen Sie das folgende Gleichungssystem im gegebenen $GF(2^5)$ und überprüfen Sie Ihr Ergebnis durch Einsetzen der berechneten Werte:

$$\begin{aligned} x + \alpha \cdot y &= \alpha^3 \\ (1 + \alpha^3) \cdot x + y &= \alpha^3 + \alpha + 1 \end{aligned}$$

e) Berechnen Sie das Generatorpolynom des gesuchten 1-Fehler-korrigierenden BCH-Codes mit den benötigten Wurzeln $\beta, \beta^2, \beta^3, \ldots, \beta^{2t}$ bezüglich des primitiven Elements α^7 des gegebenen $GF(2^5)$. Um was für einen Code handelt es sich? (Begründung!) Geben Sie die Anzahl Informationsstellen K, die Anzahl der Prüfstellen $N - K$, die Coderate R sowie die Codedistanz d des Codes an.

Beiblatt A: Mit Hilfe des Polynoms $f(D) = D^5 + D^2 + 1$ erzeugtes, erweitertes Galois-Feld $GF(2^5)$

i	$\alpha^i \bmod f(\alpha)$	i	$\alpha^i \bmod f(\alpha)$	i	$\alpha^i \bmod f(\alpha)$
0	1	11	$\alpha^2 + \alpha + 1$	22	$\alpha^4 + \alpha^2 + 1$
1	α	12		23	$\alpha^3 + \alpha^2 + \alpha + 1$
2	α^2	13		24	
3	α^3	14	$\alpha^4 + \alpha^3 + \alpha^2 + 1$	25	
4	α^4	15	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	26	$\alpha^4 + \alpha^2 + \alpha + 1$
5		16	$\alpha^4 + \alpha^3 + \alpha + 1$	27	$\alpha^3 + \alpha + 1$
6		17	$\alpha^4 + \alpha + 1$	28	$\alpha^4 + \alpha^2 + \alpha$
7	$\alpha^4 + \alpha^2$	18		29	$\alpha^3 + 1$
8	$\alpha^3 + \alpha^2 + 1$	19		30	
9	$\alpha^4 + \alpha^3 + \alpha$	20		31	1
10	$\alpha^4 + 1$	21	$\alpha^4 + \alpha^3$	32	α