Lösung 7 (Zyklische Blockcodes)

a)

$$
\begin{aligned}
& & D^N - 1 = g(D) \cdot h(D) & \\
\Rightarrow & & (D^N - 1)\ mod\ g(D) = 0 & \\
\Rightarrow & & D^N\ mod\ g(D) - 1\ mod\ g(D) = 0 & \\
\Rightarrow & & D^N\ mod\ g(D) = 1,\ da\ grad\{g(D)\} \geq 1 & \qquad (1)
\end{aligned}
$$

Weiterhin ist p die kleinste positive Zahl für die gilt:

$$
\begin{aligned}
& & D^{p+i}\ mod\ g(D) = D^i\ mod\ g(D) & \\
\Rightarrow & & D^p\ mod\ g(D) = 1,\ f\ddot{u}r\ i = 0 & \qquad (2)
\end{aligned}
$$

Formeln (1) und (2), zusammen mit der Bedingung, dass p die kleinste Zahl sein muss auf die Formel (2) zutrifft, ergeben schließlich:

$$N = p \cdot k, f\ddot{u}r\ k \geq 1,$$

d.h. p ist ein Faktor von N.

b)

$$
\begin{aligned}
D^{12} - 1 = D^{12} + 1 &= (D^3 + 1)^4 & , da\ [[f(D)]^{2^l}] = f(D^{2^l}) \\
&= (D + 1)^4 (D^2 + D + 1)^4 & , da\ D^3 + 1 = (D + 1)(D^2 + D + 1)
\end{aligned}
$$

Somit haben wir $D^N - 1$ in Faktoren irreduzibler Polynome zerlegt.

$$N - K = 12 - 7 = 5 \Rightarrow grad\{g(D)\} = 5$$

Es gibt zwei mögliche Kombinationen aus Faktoren von $D^N - 1$ welche ein Polynom vom Grad 5 erzeugen:

$$
\begin{aligned}
g_1(D) &= (D + 1)(D^2 + D + 1)^2 = D^5 + D^4 + D^3 + D^2 + D + 1 \\
g_2(D) &= (D + 1)^3 (D^2 + D + 1) = D^5 + D^3 + D^2 + 1
\end{aligned}
$$

c) Wir benötigen genausoviele unterscheidbare Syndrome wie Fehlermuster die wir korrigieren möchten. Für 1-Fehlermuster entspricht dies der Blockgröße, also $N = 12$. Weiterhin haben diese Fehlermuster die Form $e_i(D) = D^i$, wobei i die Position des Fehlers ist. Daraus ergibt sich, dass die Periode von $g(D)$ N sein muss, da ansonsten die Syndrome nicht eindeutig sind.

Beispiel: Angenommen die Periode von $g(D)$ sei 6. Dann gilt:

$$\begin{aligned} S_1(D) &= e_1(D)\ mod\ g(D) = D^1\ mod\ g(D) \\ &= D^{1+6}\ mod\ g(D) = e_7(D)\ mod\ g(D) = S_7(D), \end{aligned}$$

jeweils zwei 1-Fehlermuster führen also zu dem gleichen Syndrom. Um die Periode der beiden Kandidaten zu bestimmen, wenden wir die Bedingung $D^p\ mod\ g(D) = 1$ an. Aus a) wissen wir, dass die Periode $p \in \{1, 2, 3, 4, 6, 12\}$ gelten muss. Die Perioden $1, 2, 3$ und 4 können ausgeschlossen werden, da dann die Bedingung $D^p\ mod\ g(D) = 1$ nicht erfüllt werden kann. Überprüfen wir also, ob $g_1(D)$ oder $g_2(D)$ die Periode $p = 6$ haben könnten:

für $g_1(D)$:

$$\begin{array}{lllllll} D^6 & & & & & & :D^5+D^4+D^3+D^2+D+1=D+1 \\ D^6 & +D^5 & +D^4 & +D^3 & +D^2 & +D & \\ \hline & D^5 & +D^4 & +D^3 & +D^2 & +D & \\ & D^5 & +D^4 & +D^3 & +D^2 & +D & +1 \\ \hline & & & & & & 1 \end{array}$$

für $g_2(D)$:

$$\begin{array}{llll} D^6 & & & :D^5+D^3+D^2+1=D \\ D^6 & +D^4 & +D^3 & +D \\ \hline & D^4 & +D^3 & +D \end{array}$$

Das Generatorpolynom $g_1(D)$ hat also die Periode 6 und ist daher unzureichend. Durch Ausschluss der anderen möglichen Perioden muss $g_2(D)$ die Periode 12 besitzen.

d) Das Checkpolynom $h(D)$ ergibt sich aus den Faktoren von $D^N - 1$, welche nicht für die Konstruktion von $g_2(D)$ verwendet wurden:

$$\begin{aligned} D^{12} - 1 &= (D+1)^4(D^2+D+1)^4 \\ g_2(D) &= (D+1)^3(D^2+D+1) \\ \Rightarrow h(D) &= (D+1)(D^2+D+1)^3 = D^7 + D^5 + D^4 + D^3 + D^2 + 1 \end{aligned}$$

e)

$$
\begin{aligned}
g'(D) &= g_1(D) \cdot (D^2 + D + 1) = (D + 1)(D^2 + D + 1)^3 \\
&= D^7 + D^5 + D^4 + D^3 + D^2 + 1
\end{aligned}
$$

Es handelt sich bei $g'(D)$ um eine gültige Erweiterung von $g_1(D)$. Das Generatorpolynom lässt sich aus Faktoren von $D^N - 1$ konstruieren, somit handelt es sich um einen gültigen zyklischen Code.

f) $S(D) = e(D)\ mod\ g'(D)$

$e(D)$	$S(D)$
1	1
D	D
D^2	D^2
D^3	D^3
D^4	D^4
D^5	D^5
D^6	D^6
D^7	$D^5 + D^4 + D^3 + D^2 + 1$
D^8	$D^6 + D^5 + D^4 + D^3 + D$
D^9	$D^6 + D^3 + 1$
D^{10}	$D^5 + D^3 + D^2 + D + 1$
D^{11}	$D^6 + D^4 + D^3 + D^2 + D$

$e(D)$	$S(D)$
$D + 1$	$D + 1$
$D^2 + D$	$D^2 + D$
$D^3 + D^2$	$D^3 + D^2$
$D^4 + D^3$	$D^4 + D^3$
$D^5 + D^4$	$D^5 + D^4$
$D^6 + D^5$	$D^6 + D^5$
$D^7 + D^6$	$D^6 + D^5 + D^4 + D^3 + D^2 + 1$
$D^8 + D^7$	$D^6 + D^2 + D + 1$
$D^9 + D^8$	$D^5 + D^4 + D + 1$
$D^{10} + D^9$	$D^6 + D^5 + D^2 + D$
$D^{11} + D^{10}$	$D^6 + D^5 + D^4 + 1$
$1 + D^{11}$	$D^6 + D^4 + D^3 + D^2 + D + 1$

Alle Syndrome in der Syndromtabelle sind unterschiedlich $\Rightarrow$ die aufgeführten Fehlermuster können korrigiert werden

$$(D^9 + D^3)\ mod\ g'(D) = D^6 + 1 = (D^6 + 1)\ mod\ g'(D)$$

Die Fehlermuster $D^9 + D^3$ und $D^6 + 1$ erzeugen dasselbe Syndrom, somit können sie nicht eindeutig korrigiert werden.