Chapter 4

4.11

b) $1 + D^4 = (1 + D)^4$ in the field $\mathbb{F}_2$. We use the fact that if $C(D)$ has period T then the period T_j for $(C(D))^j$ equals $p^m T$, where p is the characteristics of the field and m a number such that $p^{m-1} < j \leq p^m$. See table.
This gives the cycle set

$$1(1) \oplus \frac{2^1 - 1}{1}(1) \oplus \frac{2^1 \cdot (2^1 - 1)}{2}(2) \oplus \frac{2^2 \cdot (2^1 - 1)}{4}(4) \oplus \frac{2^3 \cdot (2^1 - 1)}{4}(4) = \\ = 2(1) \oplus 1(2) \oplus 3(4)$$

Polynomial	Period
$1 + D$	1
$(1 + D)^2$	2
$(1 + D)^3$	4
$(1 + D)^4$	4

c) We have $1 - D - 2D^2 = (1 - 2D)^2$ in the field $\mathbb{F}_3$ with characteristic 3.
This gives the cycle set

$$1(1) \oplus \frac{3^1 - 1}{2}(2) \oplus \frac{3^1 \cdot (3^1 - 1)}{6}(6) = 1(1) \oplus 1(2) \oplus 1(6)$$

Polynomial	Period
$1 - 2D$	2
$(1 - 2D)^2$	6

4.12 We have a polynomial in the field $\mathbb{F}_{13}$ that can be factorized as

$$C(D) = 1 - 8D + 2D^2 = (1 + 10D)(1 + 8D) = C_1(D) \cdot C_2(D).$$

The polynomial $C_1(D)$ has period $T_1 = 3$ and the polynomial $C_2(D)$ has period $T_2 = 4$. We get the cycle set

$$S = S_1 \otimes S_2 = (1(1) \oplus \frac{13^1 - 1}{3}(3)) \otimes (1(1) \oplus \frac{13^1 - 1}{4}(4)) = 1(1) \oplus 3(4) \oplus 4(3) \oplus 12(12)$$

4.13 a) Find the shortest LFSR that generates $s^{(9)} = 101100001$.

n	u_n	δ_n	k	e	L	$C_n(D)$
-2						1
-1		1	-1	1	0	1
0	1	1	0	1	1	$1 + D$
1	0	1		2		1
2	1	1	2	1	2	$1 + D^2$
3	1	1		2		$1 + D + D^2$
4	0	0		3		
5	0	1	5	1	4	$1 + D + D^2 + D^3$
6	0	1		2		1
7	0	0		3		
8	1	1	8	1	5	$1 + D^3 + D^4 + D^5$

b) To generate $[s^{(9)}]^\infty$ we continue until we are back in the starting state

n	u_n	δ_n	k	e	L	$C_n(D)$
9	1	1		2		$1 + D + D^3 + D^4 + D^5$
10	0	1	10	1	6	$1 + D + D^2 + D^3 + D^4 + D^5$
11	1	1		2		$1 + D^3 + D^6$
12	1	0		3		
13	0	0		4		
14	0	0		5		

Start

$n \leftarrow -1$
$\delta_{-1} \leftarrow 1$
$C_{-2}(D) \leftarrow 1$
$C_{-1}(D) \leftarrow 1$
$L \leftarrow 0$
$k \leftarrow -1$
$e \leftarrow 1$

$n \leftarrow n + 1$

$\delta_n \leftarrow u_n - \sum_{i=1}^{L}(-c_i)u_{n-i}$

$e \leftarrow e + 1$

$\delta_n = 0$ — **Yes**

$C_n(D) \leftarrow C_{n-1}(D) - \delta_n \delta_k^{-1} D^e C_{k-1}(D)$

$n < 2L$ — **Yes**

$L \leftarrow n + 1 - L$
$k \leftarrow n$
$e \leftarrow 1$

Berlekamp–Massey algoritmen

4.14 Find an LFSR that generates $s^{(11)} =$`A60B01419BE` in $\mathbb{F}_{2^4}$.

We create $\mathbb{F}_{2^4}$ with $p(x) = x^4 + x^3 + x^2 + x + 1$. This is an irreducible polynomial since

1) $p(0) \neq 0$ and $p(1) \neq 0$ so there are no simple factors, i.e., $p(x) \neq (x - c)g(x), c \in \mathbb{F}_2$.
2) $p(x) \neq (x^2 + x + 1)h(x)$ and the given degree 2 polynomial is the only polynomial of degree 2 that is irreducible.

This shows that the polynomial $p(x)$ cannot be factored, hence, it is irreducible. Let α be a root of the polynomial $f(\alpha) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$, i.e., $\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$. To find the order of α, we know that $\text{ord}(\alpha)|p^n - 1$. Since $p^n = 2^4 = 16$ and $p^n - 1 = 16 - 1 = 15 = 1 \cdot 3 \cdot 5$ we know that $\text{ord}(\alpha) \in \{1, 3, 5, 15\}$ and we find that $\alpha^5 = 1$. Hence α is not a primitive element. (The polynomial $p(x)$ is not primitive.) We pick a new element $\beta = \alpha + 1$. We get $\beta^3 = \alpha^3 + \alpha^2 + \alpha + 1 \neq 1$ and $\beta^5 = \alpha^3 + \alpha^2 + 1 \neq 1$ so β^{15} must be one. See table.

i	β^i	polynomial				vector	
						binary	hexadecimal
$-\infty$					0	0000	0
0	β^0				1	0001	1
1	β^1			$\alpha+$	1	0011	3
2	β^2		α^2+		1	0101	5
3	β^3	α^3+	α^2+	$\alpha+$	1	1111	F
4	β^4	α^3+	α^2+	α		1110	E
5	β^5	α^3+	α^2+		1	1101	D
6	β^6	α^3				1000	8
7	β^7		α^2+	$\alpha+$	1	0111	7
8	β^8	α^3+			1	1001	9
9	β^9		α^2			0100	4
10	β^{10}	α^3+	α^2			1100	C
11	β^{11}	α^3+		$\alpha+$	1	1011	B
12	β^{12}			α		0010	2
13	β^{13}		α^2+	α		0110	6
14	β^{14}	α^3+		α		1010	A

We write the sequence $s^{(11)} =$`A60B01419BE` as $s^{(11)} = \beta^{14}\beta^{13}0\beta^{11}01\beta^{9}1\beta^{8}\beta^{11}\beta^{4}$.

Since it is an extension field over $\mathbb{F}_2$ we have that $- = +$.

n	u_n	δ_n	k	e	L	$C_n(D)$
-2						1
-1		1	-1	1	0	1
0	β^{14}	β^{14}	0	1	1	$1 - \beta^{14}1D$
1	β^{13}	0		2		
2	0	β^{12}	2	1	2	$1 - \beta^{14}D - \beta^{12}\beta^{-14}D^2 = 1 - \beta^{14}D - \beta^{13}D^2$
3	β^{11}	0		2		
4	0	β^{10}	4	1	3	$1 - \beta^{14}D - \beta^{13}D^2 - \beta^{10}\beta^{-12}D^2(1 - \beta^{14}D) = 1 - \beta^{14}D - \beta^{12}D^3$
5	1	1		2		$1 - \beta^{14}D - \beta^{12}D^3 - 1\beta^{-10}D(1 - \beta^{14}D - \beta^{13}D^2) = 1 - \beta^{7}D - \beta^{4}D^2 - \beta^{5}D^3$
6	β^9	0		3		
7	1	β^{10}	7	1	5	$1 - \beta^7D - \beta^4D^2 - \beta^5D^3 - \beta^{10}\beta^{-10}D^3(1 - \beta^{14}D - \beta^{13}D^2) =$ $1 - \beta^7D - \beta^4D^2 - \beta^{10}D^3 - \beta^{14}D^4 - \beta^{13}D^5$
8	β^8	0		2		
9	β^{11}	0		3		
10	β^4	0		4		

4.15 a)

$$S_1(D) = \frac{P_1(D)}{C_1(D)} = \frac{p_0 + p_1D + p_2D^2 + p_3D^3}{1 + D + D^4} = 1 + D^4 + \ldots \Rightarrow P_1(D) = 1 + D.$$

$$S_2(D) = \frac{P_2(D)}{C_2(D)} = \frac{p_0 + p_1D + p_2D^2}{1 + D + D^2 + D^3} = 1 + D^2 + D^4 + \ldots \Rightarrow P_2(D) = 1 + D.$$

b) No, since $\gcd(P_2(D), C_2(D)) = 1 + D$ so $S_2(D)$ can be produced by an LFSR of length two ($C_2' = 1 + D^2$).
The linear complexity of $S(D)$ is six since $\gcd(C_1(D), C_2') = 1$. So we have that $L(S_1(D) + S_2(D)) = L(S_1(D)) + L(S_2(D)) = 4 + 2$.

4.16 The sequences are of periods 14 and 7 respectively. This gives

$$s = [10000010101000]^\infty + [10100111010011]^\infty = [00100101111011]^\infty.$$

The D-transform of the sequence is

$$S(D) = \frac{P(D)}{C(D)} = \frac{D^2 + D^5 + D^7 + D^8 + D^9 + D^{10} + D^{12} + D^{13}}{1 + D^{14}}.$$

Euclid's algorithm gives that $\gcd(P(D), C(D)) = 1 + D^2 + D^4 + D^8$. Thus

$$S(D) = \frac{P'(D)}{C'(D)} = \frac{D^2 + D^4 + D^5}{1 + D^2 + D^6}.$$

The connection polynomial for the shortest LFSR is $C'(D) = 1 + D^2 + D^6$.
