ith clock tick, the entries of the shift register are shifted one place to the left, the leftmost entry a_i is output, and the next entry $a_{i+n} = \sum_{0\le j<n} f_j a_{i+j}$ of the sequence is computed by the part of the circuit consisting of arithmetic gates, and fed into the rightmost place of the shift register. Initially, the shift register is loaded with $a_0, \dots, a_{n-1}$.

It is convenient to define a multiplication of sequences by polynomials. For $f = \sum_{0\le j\le n} f_j x^j \in F[x]$ and $a = (a_i)_{i\in\mathbb{N}} \in V^{\mathbb{N}}$, we set

$$f \bullet a = \Big(\sum_{0\le j\le n} f_j a_{i+j} \Big)_{i\in\mathbb{N}} \in V^{\mathbb{N}}.$$

The constants $f \in F$ act on sequences in the usual way, and the indeterminate x acts as a shift operator:

$$x \bullet a = (a_{i+1})_{i\in\mathbb{N}}.$$

This makes $V^{\mathbb{N}}$, together with $\bullet$, into an $F[x]$-module. A module is something similar to a vector space, with the only difference that the "scalars" may be elements of an arbitrary (commutative) ring instead of a field. In particular, $\bullet$ has the following properties:

$$f \bullet (a+b) = f \bullet a + f \bullet b, \tag{1}$$
$$f \bullet \mathbf{0} = \mathbf{0}, \tag{2}$$
$$(f+g) \bullet a = f \bullet a + g \bullet a, \tag{3}$$
$$(fg) \bullet a = f \bullet (g \bullet a) = g \bullet (f \bullet a), \tag{4}$$
$$0 \bullet a = \mathbf{0}, \tag{5}$$
$$1 \bullet a = a, \tag{6}$$

for all $f, g \in F[x]$ and $a, b \in V^{\mathbb{N}}$, where $\mathbf{0} = (0)_{i\in\mathbb{N}}$ is the zero sequence. Their proof is in Exercise 12.5. For example, every commutative group G is a $\mathbb{Z}$-module by letting $f \bullet a = a^f$ for $a \in G$ and $f \in \mathbb{Z}$.

We can express the property of being a characteristic polynomial in terms of the operation $\bullet$: $f \in F[x] \setminus \{0\}$ is a characteristic polynomial of $a \in V^{\mathbb{N}}$ if and only if $f \bullet a = \mathbf{0}$. The set of all characteristic polynomials of a sequence $a \in V^{\mathbb{N}}$, together with the zero polynomial, is an ideal in $F[x]$: if f, g are both characteristic polynomials or zero, then so is $f+g$, and if $r \in F[x]$ is arbitrary, then rf is either zero or a characteristic polynomial, by (2), (3), and (4). This ideal is called the **annihilator** of a and denoted by $\mathrm{Ann}(a)$. Since any ideal in $F[x]$ is generated by a single polynomial (Section 25.3), either $\mathrm{Ann}(a) = \{0\}$ or there is a unique monic polynomial $m \in \mathrm{Ann}(a)$ of least degree such that $\langle m \rangle = \{rm : r \in F[x]\} = \mathrm{Ann}(a)$. This polynomial is called the **minimal polynomial** of a and divides any other characteristic polynomial of a. We denote it by m_a. If a is not linearly recurrent, then $\mathrm{Ann}(a) = \{0\}$, and we set $m_a = 0$. The degree of m_a is called the **recursion order** of a. Summarizing, we have the following equivalences for $f \in F[x]$ and $a \in V^{\mathbb{N}}$:

$$\begin{aligned} f = 0 \text{ or } f \text{ is a characteristic polynomial of } a &\iff f \bullet a = \mathbf{0} \\ &\iff f \in \mathrm{Ann}(a) \iff m_a \mid f, \\ a \in V^{\mathbb{N}} \text{ is linearly recurrent} &\iff \exists f \in F[x] \setminus \{0\} \quad f \bullet a = \mathbf{0} \\ &\iff \mathrm{Ann}(a) \neq \{0\} \iff m_a \neq 0. \end{aligned}$$

EXAMPLE 12.7 (continued). (i) Any polynomial annihilates the zero sequence, by (2). Thus $\mathrm{Ann}(\mathbf{0}) = F[x]$ and $m_{\mathbf{0}} = 1$.

(ii) The minimal polynomial of the Fibonacci sequence is $m_a = x^2 - x - 1$. This is because the polynomial is irreducible over $\mathbb{Q}$ (its roots $(1 \pm \sqrt{5})/2$ are irrational), and hence no proper divisor of m_a annihilates a (1 obviously does not).

(iii) The minimal polynomial of the matrix A is also the minimal polynomial of the sequence $(A^i)_{i\in\mathbb{N}}$.

(iv) m_a divides the minimal polynomial of A.

(v) m_a divides the minimal polynomial of $(A^i b)_{i\in\mathbb{N}}$.

(vi) $\mathrm{Ann}(a) \subseteq \mathrm{Ann}(\varphi(a))$ and $m_{\varphi(a)} \mid m_a$.

(vii) Let V be an algebraic field extension of F, $\alpha \in V$, and $a = (\alpha^i)_{i\ge 0}$. Then a is linearly recurrent, and the minimal polynomial of a is the minimal polynomial of α over F. $\diamond$

We now indicate how to compute the minimal polynomial of a given sequence $a = (a_i)_{i\in\mathbb{N}} \in F^{\mathbb{N}}$, provided that we know an upper bound $n \in \mathbb{N}$ on the recursion order. We recall from Section 9.1 the reversal of a polynomial: for $f = f_d x^d + \cdots + f_0 \in F[x]$ of degree d, we have

$$\mathrm{rev}(f) = \mathrm{rev}_d(f) = x^d f(x^{-1}) = f_0 x^d + f_1 x^{d-1} + \cdots + f_d \in F[x].$$

LEMMA 12.8. *Let $a = (a_i)_{i\in\mathbb{N}} \in F^{\mathbb{N}}$ be linearly recurrent, $h = \sum_{i\in\mathbb{N}} a_i x^i \in F[[x]]$, the formal power series whose coefficients are the coefficients of the sequence a, $f \in F[x] \setminus \{0\}$ of degree d, and $r = \mathrm{rev}(f)$ its reversal.*

(i) The following are equivalent.

(a) f is a characteristic polynomial of a,

(b) $r \cdot h$ is a polynomial of degree less than d,

(c) $h = g/r$ for some $g \in F[x]$ with $\deg g < d$.

(ii) If f is the minimal polynomial of a, then $d = \max\{1 + \deg g, \deg r\}$ and $\gcd(g, r) = 1$ in (i).

PROOF. For the proof of (i), see Exercise 12.7. For (ii), we note that $\deg r \le d$, with equality if and only if $x \nmid f$, and hence $d \ge \max\{1+\deg g, \deg r\}$ in (i). Now let $f = m_a$, and suppose that $d > \max\{1+\deg g, \deg r\}$. Then x divides f, $r = \mathrm{rev}(f/x)$, and f/x is a characteristic polynomial of a of degree $d-1$, by (i), contradicting the minimality of m_a. Thus $d = \max\{1+\deg g, \deg r\}$.

Let $u = \gcd(g,r)$. Then $f^* = f/\mathrm{rev}(u)$ is a polynomial of degree $d - \deg u$, $r/u = \mathrm{rev}(f^*)$, and $(r/u)h = (g/u)$ is a polynomial of degree less than $d - \deg u$. Hence f^* is a characteristic polynomial of a, again by (i), and the minimality of d implies that $\deg u = 0$. □

If $n \in \mathbb{N}$ is an upper bound on the recursion order of a, then we may compute m_a by solving the Padé approximation problem

$$h \equiv \frac{s}{t} \bmod x^{2n}, \quad x \nmid t, \quad \deg s < n, \quad \deg t \le n, \quad \gcd(s,t) = 1, \tag{7}$$

since Lemma 12.8 (ii) implies that $(s,t) = (g,r)$ is a solution to (7) (note that $x \nmid r$, by the definition of rev). We have seen in Section 5.9 that the solution to (7) is unique (up to multiplication by constants) and can be computed with the Extended Euclidean Algorithm, using $O(n^2)$ arithmetic operations in F. This leads to the following algorithm.

ALGORITHM 12.9 Minimal polynomial for $F^{\mathbb{N}}$.
Input: An upper bound $n \in \mathbb{N}$ on the recursion order and the first $2n$ entries $a_0, \ldots, a_{2n-1} \in F$ of a linearly recurrent sequence $a \in F^{\mathbb{N}}$.
Output: The minimal polynomial $m_a \in F[x]$ of a.

1. $h \longleftarrow a_{2n-1}x^{2n-1} + \cdots + a_1 x + a_0$
   call the Extended Euclidean Algorithm to compute $s,t \in F[x]$ such that $t(0) = 1$ and (7) holds, as described in Section 5.9
2. $d \longleftarrow \max\{1+\deg s, \deg t\}$, **return** $\mathrm{rev}_d(t)$

THEOREM 12.10.
Algorithm 12.9 correctly computes the minimal polynomial of a linearly recurrent sequence $(a_i)_{i\in\mathbb{N}}$ of recursion order at most n and uses $O(n^2)$ operations in F.

PROOF. Let $f \in F[x]$ be the minimal polynomial of a. The discussion preceding the algorithm implies that $(g,r) = (s,t)$, where g,r are as in Lemma 12.8 (i). Finally, $f = \mathrm{rev}_k(r)$ for some $k \in \mathbb{N}$, and Lemma 12.8 (ii) implies that $k = d$. □

Using the fast Euclidean Algorithm from Chapter 11, the minimal polynomial can actually be computed with $O(\mathsf{M}(n)\log n)$ field operations, but this does not help in our intended application.

EXAMPLE 12.11. (i) Let $F = \mathbb{F}_5$ and $a = (3,0,4,2,3,0,\ldots) \in \mathbb{F}_5^{\mathbb{N}}$ be linearly recurrent of recursion order at most 3. Then $h = 3x^4 + 2x^3 + 4x^2 + 3$ in step 1 of Algorithm 12.9, and the relevant results of the Extended Euclidean Algorithm for x^6 and h are

j	q_{j-1}	a_j	t_j
0		x^6	0
1		$3x^4+2x^3+4x^2+3$	1
2	$2x^2+2x+1$	$4x+2$	$3x^2+3x+4$
3	$2x^3+2x^2$	3	$4x^5+3x^4+x^3+2x^2+1$
4	$3x+4$	0	$3x^6$

We read off row 2 that

$$h \equiv \frac{4x+2}{3x^2+3x+4} = \frac{x+3}{2x^2+2x+1} \bmod x^6,$$

whence $s = x+3$ and $t = 2x^2+2x+1$. Finally, in step 2 we have $d = 2$ and $m_a = \mathrm{rev}_2(t) = x^2+2x+2$. We check that indeed $a_{i+2} + 2a_{i+1} + 2a_i = 0$ in $\mathbb{F}_5$ for $i = 0,1,2,3$. Thus the series continues as $(3,0,4,2,3,0,4,2,3,0,\ldots)$.

(ii) Let $a = (0,0,1,0,1,0,\ldots) \in F^{\mathbb{N}}$ of recursion order at most 3. Then $h = x^4 + x^2$, the Extended Euclidean Algorithm for x^6 and h computes

j	q_{j-1}	a_j	t_j
0		x^6	0
1		x^4+x^2	1
2	x^2-1	x^2	$-x^2+1$
3	x^2+1	0	x^4

so that $s = x^2$ and $t = -x^2+1$. Here $d = 3$ and $m_a = \mathrm{rev}_3(t) = x^3 - x$. Thus $a_{i+3} = a_{i+1}$ for all $i \ge 0$, $a_i = 0$ if i is odd, and $a_i = 1$ if $i > 0$ is even. Hence $(a_1, a_2, a_3, \ldots)$ is periodic with period 2, and a has a **preperiod** of length 1. ◇

12.4. Wiedemann's algorithm and black box linear algebra

The main idea of Wiedemann's (1986) algorithm for solving linear equations is as follows. For simplicity, we assume that $A \in F^{n\times n}$ is a nonsingular square matrix. Then for any $b \in F^n$, $y = A^{-1}b \in F^n$ is the unique solution of $Ay = b$. Suppose that $m = m_a = \sum_{0\le j\le d} m_j x^j \in F[x]$ is the minimal polynomial of the linearly recurrent sequence $a = (A^i b)_{i\in\mathbb{N}}$, that is, the unique monic polynomial of least degree such that $m \bullet a = \mathbf{0}$. Then in particular the first entry of $m \bullet a$ is zero, and

$$m(A)b = \sum_{0\le j\le d} m_j A^j b = 0 \text{ in } F^n. \tag{8}$$