Lecture 21: Linearly Recurrent Sequences

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science
rafael.oliveira.teaching@gmail.com

March 31, 2021
Overview

- Administrivia
- Linearly Recurrent Sequences
- Finding the Minimal Polynomial
- Conclusion
Rate this course!

Please log in to

https://evaluate.uwaterloo.ca/

To provide us (and the school) with your evaluation and feedback on the course!

- This would really help me figuring out what worked and what didn’t for the course
- And let the school (and santa) know if I was a good boy this term!
- Teaching this course is also a learning experience for me :)
- Administrivia

- Linearly Recurrent Sequences

- Finding the Minimal Polynomial

- Conclusion
Linearly Recurrent Sequences

**Setup:** $\mathbb{F}$ be a field, $V$ is a finite dimensional $\mathbb{F}$-vector space
Let $\mathcal{A} \equiv (a_i)_{i \in \mathbb{N}}$ be a sequence of elements $a_i \in V$
Linearly Recurrent Sequences

- **Setup:** \( \mathbb{F} \) be a field, \( V \) is a finite dimensional \( \mathbb{F} \)-vector space

  Let \( \mathcal{A} := (a_i)_{i \in \mathbb{N}} \) be a sequence of elements \( a_i \in V \)

- A sequence \( \mathcal{A} \) is **linearly recurrent** over \( \mathbb{F} \) if there are \( n \in \mathbb{N} \) and scalars \( f_0, f_1, \ldots, f_n \in \mathbb{F} \) with \( f_n \neq 0 \) such that:

  \[
  f_n a_{i+n} + f_{n-1} a_{i+n-1} + \cdots + f_0 a_i = 0 \quad \forall \ i \in \mathbb{N}
  \]

  \( a_{i+n} \) depends linearly on \( a_{i+n}, \ldots, a_i \) uniformly on \( n \) preceding terms
Linearly Recurrent Sequences

- **Setup:** \( \mathbb{F} \) be a field, \( V \) is a finite dimensional \( \mathbb{F} \)-vector space. Let \( \mathcal{A} := (a_i)_{i \in \mathbb{N}} \) be a sequence of elements \( a_i \in V \).

- A sequence \( \mathcal{A} \) is *linearly recurrent* over \( \mathbb{F} \) if there are \( n \in \mathbb{N} \) and scalars \( f_0, f_1, \ldots, f_n \in \mathbb{F} \) with \( f_n \neq 0 \) such that:

  \[
  f_n a_{i+n} + f_{n-1} a_{i+n-1} + \cdots + f_0 a_i = 0 \quad \forall \ i \in \mathbb{N}
  \]

- The polynomial

  \[
  f(x) := f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0
  \]

  is called a *characteristic* (or *annihilating*, *generating*) *polynomial* of \( \mathcal{A} \).
Examples

- \( V = \mathbb{F}^n, \ a_i = 0 \) for all \( i \in \mathbb{N} \)

Any non-zero polynomial annihilates this sequence.

\[
\begin{pmatrix}
\vec{a}_0, \vec{a}_1, \vec{a}_2, \ldots
\end{pmatrix}
\]

\( \vec{a}_0 = 1 \quad n = 0 \)
\( \vec{a}_i = 0 \)

\( \vec{f}_0 = 1 \quad \vec{f}_1 = 2 \quad n = 1 \)

\[2 \vec{a}_{2n} + \vec{a}_n = 0\]
Examples

- $V = F^n$, $a_i = 0$ for all $i \in \mathbb{N}$
  
  Any non-zero polynomial annihilates this sequence.

- $F = V = \mathbb{Q}$ and $a_{i+2} = a_{i+1} + a_i$, with $a_0 = a_1 = 1$.
  
  **Fibonacci sequence**

  $f(x) = x^2 - x - 1$ is a characteristic polynomial.

  \[ f_0 = -1 \quad f_1 = -1 \quad f_2 = 1 \quad n = 2 \]

  \[
  (1, 1, 2, 3, 5, 8, 13, 21, \ldots)
  \]
Examples

- \( V = F^n, a_i = 0 \) for all \( i \in \mathbb{N} \)
  Any non-zero polynomial annihilates this sequence.
- \( F = V = \mathbb{Q} \) and \( a_{i+2} = a_{i+1} + a_i \), with \( a_0 = a_1 = 1 \).
  Fibonacci sequence
  \[ f(x) = x^2 - x - 1 \] is a characteristic polynomial.
- \( V = \text{Mat}_n(F), A \in V \) be any matrix, \( a_i = A^i \).
  Cayley-Hamilton theorem implies that
  \[ p_A(A) = 0 \] for all \( i \in \mathbb{N} \)
  is a characteristic polynomial of \( (a_i)_{i \in \mathbb{N}} \)
\[
\begin{pmatrix}
1 & 1 \\
0 & 2
\end{pmatrix} = A \\
A^2 = \begin{pmatrix}
1 & 3 \\
0 & 4
\end{pmatrix}
\]

\[
det(tI - A) = det\left(\begin{pmatrix}
t & -1 \\
0 & t-2
\end{pmatrix}\right) = t^2 - 3t + 2
\]

\[
A^2 - 3A + 2I
\]

\[
\begin{pmatrix}
1 & 3 \\
0 & 4
\end{pmatrix} - 3 \begin{pmatrix}
1 & 1 \\
0 & 2
\end{pmatrix} + 2 \begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix} = \begin{pmatrix}
0 & 0 \\
0 & 0
\end{pmatrix}
\]
Examples

- **Krylov subspaces**

  \( V = \mathbb{F}^n, \ A \in \text{Mat}_n(\mathbb{F}) \) be any matrix and \( b \in V \). Define \( a_i = A^i b \).

  \[ p_A(t) = \det(t \cdot I - A) \]

  is a characteristic polynomial of \((a_i)_{i \in \mathbb{N}}\)

  \((b, Ab, A^2b, A^3b, \ldots)\)

  \[ p_A(A) = 0 \]

  \[ A^n \sum_{i=0}^{n} A^{-i} b = 0 \]

  \[ \sum_{i=0}^{n} f_i (A^{i+n}) = 0 \]
Examples

- **Krylov subspaces**
  
  \( V = \mathbb{F}^n, A \in \text{Mat}_n(\mathbb{F}) \) be any matrix and \( b \in V \). Define \( a_i = A^i b \).
  
  \[ p_A(t) = \det(t \cdot I - A) \]

  is a characteristic polynomial of \( (a_i)_{i \in \mathbb{N}} \)

- \( V = \mathbb{F}^n, A \in \text{Mat}_n(\mathbb{F}) \) be any matrix and \( u, b \in \mathbb{F}^n \)
  
  Define \( a_i = u^T A^i b \).
  
  \[ p_A(x) = \det(x \cdot I - A) \]

  is a characteristic polynomial of \( (a_i)_{i \in \mathbb{N}} \)
Remarks

- A linearly recurrent sequence \( A = (a_i)_{i \in \mathbb{N}} \) with a characteristic polynomial of degree \( n \) is \textit{completely determined} by its \( n \) initial values \( a_0, a_1, \ldots, a_{n-1} \).

\[
\begin{align*}
\bar{a}_0, \bar{a}_1, \ldots, \bar{a}_n \\
\end{align*}
\]

\[
\begin{align*}
\forall i \geq 0, \\
\sum_{k=0}^{n} f_k \bar{a}_{i+k} + f_{n-1} \bar{a}_{i+n-1} + \ldots + f_0 \bar{a}_i = 0
\end{align*}
\]
Remarks

- A linearly recurrent sequence $A = (a_i)_{i \in \mathbb{N}}$ with a characteristic polynomial of degree $n$ is \textit{completely determined} by its $n$ initial values $a_0, a_1, \ldots, a_{n-1}$.

- Given enough initial values and characteristic polynomial, can compute the $m^{th}$ term in $O(m)$ operations.

\[ a_0, a_1, a_{n-1}, a_n, a_{n+1}, a_m \]

It $\pi$ operations each time

\[ O(m) \]
Remarks

- A linearly recurrent sequence $A = (a_i)_{i \in \mathbb{N}}$ with a characteristic polynomial of degree $n$ is *completely determined* by its $n$ initial values $a_0, a_1, \ldots, a_{n-1}$.

- Given enough initial values and characteristic polynomial, can compute the $m^{th}$ term in $O(m)$ operations.

- A linear recurrent sequence $A$ has *infinitely many* valid characteristic polynomials!

  Fibonacci sequence. Let $f(x) = x^2 - x - 1$ and $g(x) = x - 1$, then

  $$h(x) = f(x) \cdot g(x)$$

  is another characteristic polynomial!
\[ a_{i+2} - a_{i+1} - a_i = 0 \]

\[ f(x) = x^2 - x - 1 \]

\[ x \circ a_i \mapsto a_{i+1} \]

\[ x^2 \circ a_i \mapsto x \circ a_{i+1} \mapsto a_{i+2} \]

\[ f \circ a_i = (x^2 - x - 1) \circ a_i = -a_i - a_{i+1} + a_{i+2} \]
Minimal Polynomial

- A linear recurrent sequence $\mathcal{A}$ has \textit{infinitely many} valid characteristic polynomials!

Fibonacci sequence. Let $f(x) = x^2 - x - 1$ and $g(x) = x - 1$, then

$$h(x) = f(x) \cdot g(x)$$

is another characteristic polynomial!

\[
g(x) \cdot f(x) = (x-1)(x^2-x-1) = x(x^2-x-1) - (x^2-x-1)
\]

\[
\begin{align*}
&h_3 a_{i+3} + h_2 a_{i+2} + h_1 a_{i+1} + h_0 a_i = 0 \\
&(a_{i+2} - a_{i+1} - q_{i+1}) - (a_{i+1} - a_{i} - q_i) = 0
\end{align*}
\]

$h$ is also char. poly.
Minimal Polynomial

- A linear recurrent sequence \( \mathcal{A} \) has \textit{infinitely many} valid characteristic polynomials!
  
  Fibonacci sequence. Let \( f(x) = x^2 - x - 1 \) and \( g(x) = x - 1 \), then
  
  \[ h(x) = f(x) \cdot g(x) \]
  
  is another characteristic polynomial!

- Note that if \( f(x), h(x) \) are characteristic polynomials, so is \( f + h \)
Minimal Polynomial

- A linear recurrent sequence $\mathcal{A}$ has *infinitely many* valid characteristic polynomials!

Fibonacci sequence. Let $f(x) = x^2 - x - 1$ and $g(x) = x - 1$, then

$$h(x) = f(x) \cdot g(x)$$

is another characteristic polynomial!

- Note that if $f(x)$, $h(x)$ are characteristic polynomials, so is $f + h$

- Given linearly recurrent sequence $\mathcal{A} = (a_i)_{i \in \mathbb{N}}$

$$Ann(\mathcal{A}) := \{f(x) \in \mathbb{F}[x] \mid f \text{ is characteristic polynomial of } \mathcal{A}\} \cup \{0\}$$

$Ann(\mathcal{A})$ is an *ideal* of $\mathbb{F}[x]$. 
Minimal Polynomial

- A linear recurrent sequence $\mathcal{A}$ has \textit{infinitely many} valid characteristic polynomials!
  - Fibonacci sequence. Let $f(x) = x^2 - x - 1$ and $g(x) = x - 1$, then
    \[ h(x) = f(x) \cdot g(x) \]
    is another characteristic polynomial!

- Note that if $f(x), h(x)$ are characteristic polynomials, so is $f + h$

- Given linearly recurrent sequence $\mathcal{A} = (a_i)_{i \in \mathbb{N}}$
  
  $$\text{Ann}(\mathcal{A}) := \{ f(x) \in \mathbb{F}[x] \mid f \text{ is characteristic polynomial of } \mathcal{A} \} \cup \{0\}$$

  $\text{Ann}(\mathcal{A})$ is an \textit{ideal} of $\mathbb{F}[x]$.

- $\mathbb{F}[x]$ is a PID. Thus, there exists \textit{non-zero, monic} $p_\mathcal{A}(x) \in \mathbb{F}[x]$ such that
  \[ \text{Ann}(\mathcal{A}) = (p_\mathcal{A}(x)) \]
  $p_\mathcal{A}(x)$ is called the \textit{minimal polynomial} of $\mathcal{A}$
Examples

- \( V = \mathbb{F}^n, a_i = 0 \) for all \( i \in \mathbb{N} \)
  
  Any non-zero polynomial annihilates this sequence.
  
  Thus, \( p_A(x) = 1 \) and \( \text{Ann}(A) = \mathbb{F}[x] \)
Examples

- $V = \mathbb{F}^n$, $a_i = 0$ for all $i \in \mathbb{N}$

  Any non-zero polynomial annihilates this sequence.

  Thus, $p_A(x) = 1$ and $\text{Ann}(A) = \mathbb{F}[x]$.

- $\mathbb{F} = V = \mathbb{Q}$ and $a_{i+2} = a_{i+1} + a_i$, with $a_0 = a_1 = 1$.

  **Fibonacci sequence**

  $f(x) = x^2 - x - 1$ is the minimal polynomial.

  $x - \alpha \mid f(x) \iff f(\alpha) = 0$

  $\alpha \in \mathbb{Q}$

  \[
  \frac{1 \pm \sqrt{5}}{2}
  \]

  Not rational roots of $f(x)$
Examples

- \( V = \mathbb{F}^n, \ a_i = 0 \) for all \( i \in \mathbb{N} \)
  
  Any non-zero polynomial annihilates this sequence.

  Thus, \( p_A(x) = 1 \) and \( \text{Ann}(A) = \mathbb{F}[x] \)

- \( \mathbb{F} = V = \mathbb{Q} \) and \( a_{i+2} = a_{i+1} + a_i \), with \( a_0 = a_1 = 1 \).

  **Fibonacci sequence**

  \( f(x) = x^2 - x - 1 \) is the minimal polynomial.

- \( V = \text{Mat}_n(\mathbb{F}), \ M \in V \) be any matrix, \( a_i = M^i \).

  Cayley-Hamilton implies \( p_M(x) = \det(x \cdot I - M) \) is a characteristic polynomial.

  Situation here is more subtle.
Examples

- \( V = \text{Mat}_n(\mathbb{F}) \), \( M \in V \) be any matrix, \( a_i = M^i \).
- \( n = 3 \), \( M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \) is not the minimal polynomial.
- \( p_M(x) = x^3 \) is the minimal polynomial.
- \( p_M(x) = \det(xI - M) = x^3 \)
- \( M^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \)
- \( \text{Ann}(A) = (x^2) \) is not the minimal polynomial.
- \( \text{Ann}(A) = (x-1)^3 \) is the minimal polynomial.
Examples

- $V = \text{Mat}_n(\mathbb{F})$, $M \in V$ be any matrix, $a_i = M^i$.

- $n = 3$, $M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$

  $p_M(x) = x^3$ is the minimal polynomial

- $n = 3$, $M = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

  $p_M(x) = x^3$ is \textit{not} the minimal polynomial. $\text{Ann}(A) = (x^2)$
Examples

- $V = \text{Mat}_n(\mathbb{F})$, $M \in V$ be any matrix, $a_i = M^i$.
- $n = 3$, $M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$

\[ p_M(x) = x^3 \text{ is the minimal polynomial} \]

- $n = 3$, $M = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

\[ p_M(x) = x^3 \text{ is not the minimal polynomial. } \text{Ann}(A) = (x^2) \]

- $n = 3$, $M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

\[ p_M(x) = (x - 1)^3 \text{ is not the minimal polynomial. } \text{Ann}(A) = (x - 1) \]
Examples

- $V = \text{Mat}_n(\mathbb{F})$, $M \in V$ be any matrix, $a_i = M^i$.

- $n = 3$, $M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$

  $p_M(x) = x^3$ is the minimal polynomial.

- $n = 3$, $M = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

  $p_M(x) = x^3$ is not the minimal polynomial. $\text{Ann}(A) = (x^2)$

- $n = 3$, $M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

  $p_M(x) = (x - 1)^3$ is not the minimal polynomial. $\text{Ann}(A) = (x - 1)$

- $n = 3$, $M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$

  $\text{Ann}(A) = (((x - 1)(x - 2)(x - 3)))$ is the minimal polynomial.
Examples

- **Krylov subspaces**

  \[ V = \mathbb{F}^n, \ M \in \text{Mat}_n(\mathbb{F}) \] be any matrix and \( b \in V \). Define \( a_i = M^i b \).

  Have two sequences \( A = (a_i)_{i \in \mathbb{N}} \) and \( B = (M^i)_{i \in \mathbb{N}} \).

  \[ p_A(x) \] may not be minimal polynomial of \( B \).

  \[ Q: \text{will it be the case the minimal polynomial } \]

  \[ p_B = p_A ? \]

  \[ \text{NO.} \]

  \[ \text{all we can say } \]

  \[ |p_A| \neq |p_B| \]
Examples

- **Krylov subspaces**

  \( V = \mathbb{F}^n, \ M \in \text{Mat}_n(\mathbb{F}) \) be any matrix and \( \mathbf{b} \in V \). Define \( \mathbf{a}_i = M^i \mathbf{b} \).

  Have two sequences \( \mathcal{A} = (\mathbf{a}_i)_{i \in \mathbb{N}} \) and \( \mathcal{B} = (M^i)_{i \in \mathbb{N}} \).

- \( n = 3, \ M = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \ b = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \)

  \( \text{Ann}(\mathcal{B}) = (x^2) \) whereas \( \text{Ann}(\mathcal{A}) = \mathbb{F}[x] = (1) \)

  \[ M^i \mathbf{b} = \mathbf{0} \]
Examples

- **Krylov subspaces**

  \( V = \mathbb{F}^n, M \in \text{Mat}_n(\mathbb{F}) \) be any matrix and \( b \in V \). Define \( a_i = M^i b \).

  Have two sequences \( \mathcal{A} = (a_i)_{i \in \mathbb{N}} \) and \( \mathcal{B} = (M^i)_{i \in \mathbb{N}} \).

- \( n = 3, M = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \)

  \( \text{Ann}(\mathcal{B}) = (x^2) \) whereas \( \text{Ann}(\mathcal{A}) = \mathbb{F}[x] \)

- \( n = 3, M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \)

  \( \text{Ann}(\mathcal{B}) = (x^2) = \text{Ann}(\mathcal{A}) \)

  \( \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \ldots \)

  \( O_{i+2} = 0 \) ; \( A_i \nabla O \)
Examples

- **Krylov subspaces**

  \(V = \mathbb{F}^n, \ M \in \text{Mat}_n(\mathbb{F})\) be any matrix and \(b \in V\). Define \(a_i = M^i b\).

  Have two sequences \(A = (a_i)_{i \in \mathbb{N}}\) and \(B = (M^i)_{i \in \mathbb{N}}\).

- \(n = 3, \ M = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \ b = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}\)

  \(\text{Ann}(B) = (x^2)\) whereas \(\text{Ann}(A) = \mathbb{F}[x]\)

- \(n = 3, \ M = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \ b = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\)

  \(\text{Ann}(B) = (x^2) = \text{Ann}(A)\)

- \(n = 3, \ M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \ b = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}\)

  \(\text{Ann}(B) = (x^3)\) whereas \(\text{Ann}(A) = (x^2)\)
Administrivia

Linearly Recurrent Sequences

Finding the Minimal Polynomial

Conclusion
Computing the Minimal Polynomial

- **For this part of the lecture,** \( V = \mathbb{F} \)
- **Input:** bound \( n \in \mathbb{N} \) on the degree of the minimal polynomial, initial terms \( a_0, \ldots, a_{2n-1} \in \mathbb{F} \)
- **Output:** minimal polynomial for the sequence \( A = (a_i)_{i \in \mathbb{N}} \)

\[
A = (a_i)_{i \in \mathbb{N}}
\]

\[
h_c(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots \in \mathbb{F}[x]
\]

\[
l(x) = f_0 + f_1 x + \ldots + f_d x^d \iff \text{rev}_d(l) = x^d l(x^{-1}) = f_0 x^d + f_1 x^{d-1} + \ldots + f_d
\]
Computing the Minimal Polynomial

- For this part of the lecture, \( V = \mathbb{F} \)
- **Input:** bound \( n \in \mathbb{N} \) on the degree of the minimal polynomial, initial terms \( a_0, \ldots, a_{2n-1} \in \mathbb{F} \)
- **Output:** minimal polynomial for the sequence \( A = (a_i)_{i \in \mathbb{N}} \)

The following lemma gives us equivalent ways of describing characteristic polynomials

**Lemma (Description of Characteristic Polynomials)**

Let \( A = (a_i)_{i \in \mathbb{N}} \) be our sequence, \( h(x) = \sum_{i \geq 0} a_i x^i \) be the formal power series defined by \( A \), \( f(x) \in \mathbb{F}[x] \) non-zero of degree \( d \) and \( r(x) = \text{rev}_d(f) \) be the reversal of \( f \). The following are equivalent:

1. \( f \in \text{Ann}(A) \) \( \quad \) \( f \) is characteristic polynomial
2. \( r \cdot h \) is a polynomial of degree \(< d \)

Moreover, if \( f(x) \) is the minimal polynomial of \( A \), then

\[
d = \max\{1 + \deg(g), \deg r\} \quad \text{and} \quad \gcd(g, r) = 1
\]
Characterizing Minimal Polynomial

- (1) \(\Rightarrow\) (2): we know that \(f(x)\) is a minimal polynomial.

Compute coefficient of \(x^{d+k}\) of the power series \(h(x) \cdot r(x)\)

\[f(x) = f_d x^d + f_{d-1} x^{d-1} + \cdots + f_0\]
\[r(x) = r_d + r_{d-1} x + \cdots + r_0 x^d\]

\[
\begin{bmatrix}
[h \cdot r]
\end{bmatrix}_{d+k} = 
\begin{bmatrix}
(a_0 + a_1 x + \cdots + a_{d+k}) (f_d + f_{d-1} x + \cdots + f_0 x^{d})
\end{bmatrix}_{d+k}
\]

\[
= f_d \cdot a_{d+k} + f_{d-1} \cdot a_{d+k-1} + f_{d-2} \cdot a_{d+k-2} + \cdots + f_0 \cdot a_n
\]

\[\{\text{characteristic}\Rightarrow f_d a_{d+m} + \cdots + f_0 a_n = 0 \quad \forall n \geq 0\]
\[\Rightarrow [h \cdot r]_{d+k} = 0 \quad \forall k \geq 0\]
Characterizing Minimal Polynomial

• (1) ⇒ (2): we know that \( f(x) \) is a minimal polynomial.
  
  Compute coefficient of \( x^{d+k} \) of the power series \( h(x) \cdot r(x) \)

• (2) ⇒ (1): we know that \( h \cdot r \) is a polynomial of degree \( < d = \deg(f) \)
  
  Compute coefficient of \( x^{d+k} \) of the power series \( h(x) \cdot r(x) \)

\[
\theta = [h \cdot r]_{d+k} = f_d a_d x^n + f_{d-1} a_{d-1} x^{n-1} + \ldots + f_0 a_n
\]

\( f(x) \) is characteristic polynomial.
Characterizing Minimal Polynomial

- $(1) \Rightarrow (2)$: we know that $f(x)$ is a minimal polynomial.
  
  Compute coefficient of $x^{d+k}$ of the power series $h(x) \cdot r(x)$

- $(2) \Rightarrow (1)$: we know that $h \cdot r$ is a polynomial of degree $< d = \deg(f)$
  
  Compute coefficient of $x^{d+k}$ of the power series $h(x) \cdot r(x)$

- Moreover part: if $f$ is the minimal polynomial,

  
  $$d = \max\{1 + \deg(g), \deg r\} \quad \text{and} \quad \gcd(g, r) = 1$$
Characterizing Minimal Polynomial

\[ \deg(g) < \deg(f) = d \]
\[ \deg(\alpha) = d \]
\[ \pi(x) = x^d \cdot \varphi(x) \]

Moreover part: if \( f \) is the minimal polynomial,

\[ d = \max\{1 + \deg(g), \deg r\} \quad \text{and} \quad \gcd(g, r) = 1 \]

\[ d = \max\{1 + \deg(g), \deg r\} \] holds by definition of reversal and the fact that \( f \) is a characteristic polynomial
Characterizing Minimal Polynomial

\[ h \cdot r = g \]
\[ h \cdot \frac{x}{q} = \left(\frac{g}{q}\right) \]

Moreover part: if \( f \) is the minimal polynomial,

\[ d = \max\{1 + \deg(g), \deg r\} \quad \text{and} \quad \gcd(g, r) = 1 \]

if \( \gcd(g, r) = q(x) \neq 1 \), let \( e = \deg(q) \). Then \( \text{rev}_{d-e}(r/q) \) is also a characteristic polynomial, since

\[ \text{rev}_{d-e}(\text{rev}_{d-e}(r/q)) = r/q \]

and the first part of lemma.
Computing the Minimal Polynomial

- Lemma gives us a way to compute minimal polynomial from power series expansion.

  Given $h$ and $n$, all we need to do is find $r, g$ such that $\deg(r) \leq n$, $\deg(g) < n$, $\gcd(r, g) = 1$ and $rh = g$.

\[ \text{Padé approximation problem:} \quad h \equiv g_r \mod x^n, \quad x \nmid r \]

\[ \deg(g) < n, \quad \deg(r) \leq n, \quad \gcd(r, g) = 1 \]

Why would a solution mod $x^n$ be good?

If $A$ is a linearly recurrence sequence of order $n$, then system above gives us at least $n$ relations that $\text{rev}(r)$ will satisfy, so it is a characteristic polynomial!

How to solve it?

Linear system of equations + Euclidean Algorithm!

\[ 1 \]

There is a more efficient way to do this, by using only the EEA.
Computing the Minimal Polynomial

- Lemma gives us a way to compute minimal polynomial from power series expansion.
  
  Given $h$ and $n$, all we need to do is find $r, g$ such that $\deg(r) \leq n$, $\deg(g) < n$, $\gcd(r, g) = 1$ and $rh = g$.

- Padé approximation problem:
  
  $$h \equiv \frac{g}{r} \mod x^{2n}, \quad x \nmid r \quad \deg(g) < n, \quad \deg(r) \leq n, \quad \gcd(r, g) = 1$$

  \[ x_0 \neq 0 \]
  \[ (x_0 = 1) \]

\[ ^1 \text{There is a more efficient way to do this, by using only the EEA.} \]
Lemma gives us a way to compute minimal polynomial from power series expansion.

Given $h$ and $n$, all we need to do is find $r, g$ such that $\deg(r) \leq n$, $\deg(g) < n$, $\gcd(r, g) = 1$ and $rh = g$.

Padé approximation problem:

$$h \equiv \frac{g}{r} \mod x^{2n}, \quad x \nmid r \quad \deg(g) < n, \quad \deg(r) \leq n, \quad \gcd(r, g) = 1$$

Why would a solution $\mod x^{2n}$ be good?

If $A$ is a linearly recurrence sequence of order $n$, then system above gives us at least $n$ relations that $\text{rev}_n(r)$ will satisfy, so it is a characteristic polynomial!

$Q_0, Q_1, Q_2, \ldots, Q_{n-1}, Q_n, Q_{n+1}, \ldots, Q_{2n}$

\[1\] There is a more efficient way to do this, by using only the EEA.
Computing the Minimal Polynomial

- Lemma gives us a way to compute minimal polynomial from power series expansion.
  
  Given $h$ and $n$, all we need to do is find $r, g$ such that $\deg(r) \leq n$, $\deg(g) < n$, $\gcd(r, g) = 1$ and $rh = g$.

- Padé approximation problem:

  $$ h \equiv \frac{g}{r} \mod x^{2n}, \quad x \nmid r \quad \deg(g) < n, \quad \deg(r) \leq n, \quad \gcd(r, g) = 1 $$

- Why would a solution $\mod x^{2n}$ be good?

  If $\mathcal{A}$ is a linearly recurrence sequence of order $n$, then system above gives us at least $n$ relations that $\text{rev}(r)$ will satisfy, so it is a characteristic polynomial!

- How to solve it?

  Linear system of equations + Euclidean Algorithm!\(^1\)

\(^1\)There is a more efficient way to do this, by using only the EEA.
Algorithm

- **Input:** bound $n \in \mathbb{N}$ on the degree of the minimal polynomial, initial terms $a_0, \ldots, a_{2n-1} \in F$
- **Output:** the minimal polynomial for the sequence $A = (a_i)_{i \in \mathbb{N}}$
Algorithm

\[
\begin{align*}
\text{Input:} & \quad \text{bound } n \in \mathbb{N} \text{ on the degree of the minimal polynomial, initial terms } a_0, \ldots, a_{2n-1} \in \mathbb{F} \\
\text{Output:} & \quad \text{the minimal polynomial for the sequence } A = (a_i)_{i \in \mathbb{N}} \\
\text{Find } g, r \in \mathbb{F}[x] & \text{ that solve the following system:} \\
h & \equiv \frac{g}{r} \mod x^{2n}, \quad x \not| r, \quad \deg(g) < n, \quad \deg(r) \leq n, \quad \gcd(r, g) = 1
\end{align*}
\]

\[
\begin{align*}
h(x) &= a_0 + a_1 x + a_2 x^2 + \cdots + a_{2n-1} x^{2n-1} \mod x^{2n} \\
g(x) &= g_0 + g_1 x + g_2 x^2 + \cdots + g_{2n-1} x^{2n-1} \\
\pi(x) &= 1 + \pi_1 x + \pi_2 x^2 + \cdots + \pi_n x^n
\end{align*}
\]

\[\pi \equiv \frac{g}{\gcd} \quad \hat{g} = \frac{g}{\gcd}\]
Algorithm

- **Input:** bound $n \in \mathbb{N}$ on the degree of the minimal polynomial, initial terms $a_0, \ldots, a_{2n-1} \in \mathbb{F}$
- **Output:** the minimal polynomial for the sequence $A = (a_i)_{i \in \mathbb{N}}$

1. Find $g, r \in \mathbb{F}[x]$ that solve the following system:

$$h \equiv \frac{g}{r} \mod x^{2n}, \quad x \nmid r \quad \deg(g) < n, \quad \deg(r) \leq n, \quad \gcd(r, g) = 1$$

2. Set $d = \max\{1 + \deg(g), \deg(r)\}$
3. Return $rev_d(r)$
Algorithm

- **Input:** bound $n \in \mathbb{N}$ on the degree of the minimal polynomial, initial terms $a_0, \ldots, a_{2n-1} \in \mathbb{F}$
- **Output:** the minimal polynomial for the sequence $A = (a_i)_{i \in \mathbb{N}}$

1. Find $g, r \in \mathbb{F}[x]$ that solve the following system:
   \[
   h \equiv \frac{g}{r} \mod x^{2n}, \quad x \nmid r \quad \deg(g) < n, \quad \deg(r) \leq n, \quad \gcd(r, g) = 1
   \]

2. Set $d = \max\{1 + \deg(g), \deg(r)\}$
3. Return $\text{rev}_d(r)$

- The efficient version to solve the system above performs $O(M(n) \log n)$ operations in $\mathbb{F}$, where $M(n)$ is the time it takes to multiply two degree $n$ polynomials.
Conclusion

- Today we learned about linearly recurrent sequences
- Learned about the minimal polynomial of a linearly recurrent sequence and how to compute it
- Next lecture: see how linearly recurrent sequences appear naturally in linear algebra
- Unfortunately, even the fast version of the algorithm of today will not be good enough for next lecture...

  Good news: we will devise faster algorithms!
von zur Gathen, J. and Gerhard, J. 2013. Modern Computer Algebra
Cambridge University Press

Chapter 12