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

Linearly Recurrent Sequences

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

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

$$\underbrace{f_n}_{\neq 0}\mathbf{a}_{i+n} + \underline{f_{n-1}}\mathbf{a}_{i+n-1} + \cdots + \underline{f_0}\mathbf{a}_i = 0 \quad \forall\, i \in \mathbb{N}$$

a_{i+n} depends $\underbrace{\ }_{\text{uniformly}}$ linearly on $\underbrace{a_{i+n-1}, \ldots, a_i}_{n \text{ preceding terms}}$

Linearly Recurrent Sequences

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

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

- 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:

$$f_n\mathbf{a}_{i+n} + f_{n-1}\mathbf{a}_{i+n-1} + \cdots + f_0\mathbf{a}_i = 0 \;\; \forall\, i \in \mathbb{N}$$

- 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

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

  Any non-zero polynomial annihilates this sequence.

$$(\vec{0}, \vec{0}, \vec{0}, \vec{0}, \vec{0}, \dots)$$

$$\boxed{f_0 = 1 \qquad n = 0}$$

$$\vec{a}_i = 0$$

$$\boxed{f_0 = 1 \quad f_1 = 2 \qquad n = 1}$$

$$2\vec{a}_{i+1} + \vec{a}_i = 0$$

Examples

$a_{i+2} - a_{i+1} - a_i = 0$

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

  Any non-zero polynomial annihilates this sequence.

- $\mathbb{F} = V = \mathbb{Q}$ and $\boxed{\mathbf{a}_{i+2} = \mathbf{a}_{i+1} + \mathbf{a}_i}$, with $\mathbf{a}_0 = \mathbf{a}_1 = 1$.

  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

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

  Any non-zero polynomial annihilates this sequence.

- $\mathbb{F} = V = \mathbb{Q}$ and $\mathbf{a}_{i+2} = \mathbf{a}_{i+1} + \mathbf{a}_i$, with $\mathbf{a}_0 = \mathbf{a}_1 = 1$.

  Fibonacci sequence

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

- $V = \mathrm{Mat}_n(\mathbb{F})$, $A \in V$ be any matrix, $\mathbf{a}_i = A^i$.

  $P_A(A) = 0$

  Cayley-Hamilton theorem implies that

  $$p_A(x) = \det(x \cdot I - A)$$

  is a characteristic polynomial of $(\mathbf{a}_i)_{i \in \mathbb{N}}$

  $(I, A, A^2, A^3, \ldots)$

$$\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} = A \qquad A^2 = \begin{pmatrix} 1 & 3 \\ 0 & 4 \end{pmatrix}$$

$$\det(tI - A) = \det\begin{pmatrix} t-1 & -1 \\ 0 & t-2 \end{pmatrix} =$$

$$= t^2 - 3t + 2$$

$$A^2 - 3A + 2 \cdot I$$

$$\begin{pmatrix} 1 & 3 \\ 0 & 4 \end{pmatrix} - 3\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} + 2\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Examples

- *Krylov subspaces*

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

$$p_A(t) = \underline{\det(t \cdot I - A)}$$

is a characteristic polynomial of $(\mathbf{a}_i)_{i\in\mathbb{N}}$

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

$$p_A(A) = 0 \qquad \text{Cayley-Hamilton}$$

$$A^n \sum_{i=0}^{n} A^{i+n} \cdot f_i = 0 \cdot A^n$$

$$\sum_{i=0}^{n} f_i \cdot (A^{i+n} b) = 0$$

$$\vec{a}_{i+n}$$

Examples

- *Krylov subspaces*

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

$$p_A(t) = \det(t \cdot I - A)$$

is a characteristic polynomial of $(\mathbf{a}_i)_{i\in\mathbb{N}}$

- $V = \mathbb{F}^n$, $A \in \mathrm{Mat}_n(\mathbb{F})$ be any matrix and $\mathbf{u}, \mathbf{b} \in \mathbb{F}^n$.

  Define $\mathbf{a}_i = \mathbf{u}^T A^i \mathbf{b}$.

$$p_A(x) = \det(x \cdot I - A)$$

is a characteristic polynomial of $(\mathbf{a}_i)_{i\in\mathbb{N}}$

Remarks

- A linearly recurrent sequence $\mathcal{A} = (\mathbf{a}_i)_{i \in \mathbb{N}}$ with a characteristic polynomial of degree n is *completely determined* by its n initial values

$$\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{n-1}$$

$$\boxed{\vec{a}_0, \vec{a}_1, \ldots, \vec{a}_{n-1}}$$

$$f(x) = f_n x^n + \cdots + f_0$$

$i \geq 0$

$$\underbrace{f_n}_{\neq 0} \vec{a}_{i+n} + f_{n-1} \vec{a}_{i+n-1} + \cdots + f_0 \vec{a}_i = 0$$

Remarks

- A linearly recurrent sequence $\mathcal{A} = (\mathbf{a}_i)_{i\in\mathbb{N}}$ with a characteristic polynomial of degree n is *completely determined* by its n initial values

$$\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{n-1}$$

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

$$\vec{a}_0 \quad \vec{a}_1 \quad \cdot \quad \vec{a}_{n-1} \quad \underbrace{\vec{a}_n \quad \vec{a}_{n+1} \qquad \vec{a}_m}_{\text{1+n operations each time}}$$

n constant

$O(m)$

Remarks

- A linearly recurrent sequence $\mathcal{A} = (\mathbf{a}_i)_{i \in \mathbb{N}}$ with a characteristic polynomial of degree n is *completely determined* by its n initial values

$$\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{n-1}$$

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

$$\boxed{a_{i+2} - a_{i+1} - a_i = 0}$$

$$f(x) = x^2 - x - 1$$

$$x \circ a_i \longmapsto a_{i+1}$$

$$x^2 \circ a_i \longmapsto x \circ a_{i+1} \longmapsto a_{i+2}$$

$$f \circ a_i = (x^2 - x - 1) \circ a_i = -a_i - a_{i+1} + a_{i+2}$$

Minimal Polynomial

- A linear recurrent sequence $\mathcal{A}$ has *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!

$$\boxed{h_0 a_i}$$

$$h(x) = g(x)\,\underline{f(x)} = (x-1)(x^2-x-1)$$

$$= \underline{x(x^2-x-1)} - \underline{(x^2-x-1)}$$

$$\boxed{h_3 a_{i+3} + h_2 a_{i+2} + h_1 a_{i+1} + h_0 a_i = 0}$$

$$(a_{i+3} - a_{i+2} - a_{i+1}) - \underbrace{(a_{i+2} - a_{i+1} - a_i)}_{=0} = 0$$

$$= 0$$

$\therefore$ h is also char. poly.

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 $f + h$

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 $\boxed{f + h}$
- Given linearly recurrent sequence $\mathcal{A} = (\mathbf{a}_i)_{i \in \mathbb{N}}$

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

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

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 $\mathcal{A} = (\mathbf{a}_i)_{i \in \mathbb{N}}$

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

  $Ann(\mathcal{A})$ is an *ideal* of $\mathbb{F}[x]$.
- $\mathbb{F}[x]$ is a PID. Thus, there exists *non-zero*, *monic* $p_{\mathcal{A}}(x) \in \mathbb{F}[x]$ such that

  $$Ann(\mathcal{A}) = (p_{\mathcal{A}}(x))$$

  $p_{\mathcal{A}}(x)$ is called the *minimal polynomial* of $\mathcal{A}$

Examples

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

  Any non-zero polynomial annihilates this sequence.

  Thus, $p_{\mathcal{A}}(x) = 1$ and $Ann(\mathcal{A}) = \mathbb{F}[x]$

Examples

$a_1 - \alpha a_0 = 0$

$\boxed{\alpha = 1}$ cont.

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

  Any non-zero polynomial annihilates this sequence.

  Thus, $p_{\mathcal{A}}(x) = 1$ and $Ann(\mathcal{A}) = \mathbb{F}[x]$
- $\mathbb{F} = V = \mathbb{Q}$ and $\mathbf{a}_{i+2} = \mathbf{a}_{i+1} + \mathbf{a}_i$, with $\mathbf{a}_0 = \mathbf{a}_1 = 1$.

  $\mathbb{R}$

  Fibonacci sequence

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

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

$\alpha \in \mathbb{Q}$

$\underbrace{\frac{1 \pm \sqrt{5}}{2}}_{\text{not rational}}$ roots of $f(x)$

Examples

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

  Any non-zero polynomial annihilates this sequence.

  Thus, $p_{\mathcal{A}}(x) = 1$ and $Ann(\mathcal{A}) = \mathbb{F}[x]$
- $\mathbb{F} = V = \mathbb{Q}$ and $\mathbf{a}_{i+2} = \mathbf{a}_{i+1} + \mathbf{a}_i$, with $\mathbf{a}_0 = \mathbf{a}_1 = 1$.

  Fibonacci sequence

  $f(x) = x^2 - x - 1$ is the minimal polynomial.
- $V = \mathrm{Mat}_n(\mathbb{F})$, $M \in V$ be any matrix, $\mathbf{a}_i = M^i$.

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

  Situation here is more subtle.

Examples

- $V = \mathrm{Mat}_n(\mathbb{F})$, $M \in V$ be any matrix, $\mathbf{a}_i = M^i$.
- $n = 3$, $M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ $\qquad \cancel{x} \quad \cancel{x^2}$

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

$$p_M(x) = \det(xI - M) = \underline{x^3}$$

$$M^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Examples

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

  $p_M(x) = x^3$ 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. $Ann(\mathcal{A}) = (x^2)$

Examples

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

  $p_M(x) = x^3$ 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. $Ann(\mathcal{A}) = (x^2)$
- $n = 3,\ M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

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

Examples

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

  $p_M(x) = x^3$ 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. $Ann(\mathcal{A}) = (x^2)$
- $n = 3,\ M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

  $p_M(x) = (x-1)^3$ is *not* the minimal polynomial. $Ann(\mathcal{A}) = (x-1)$
- $n = 3,\ M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$

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

Examples

- *Krylov subspaces*

  $V = \mathbb{F}^n$, $M \in \mathrm{Mat}_n(\mathbb{F})$ 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 $\mathcal{B} = (M^i)_{i\in\mathbb{N}}$.

$p_M(x)$ may not be minimal polynomial of $\mathcal{B}$

Q: will it be the case the minimal polynomial $p_{\mathcal{B}} = p_{\mathcal{A}}$?

NO.

$\boxed{p_{\mathcal{A}} \mid p_{\mathcal{B}}}$. all we can say

Examples

- *Krylov subspaces*

  $V = \mathbb{F}^n$, $M \in \mathrm{Mat}_n(\mathbb{F})$ 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 $\mathcal{B} = (M^i)_{i \in \mathbb{N}}$.

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

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

$M^i b = \vec{0}$

Examples

- *Krylov subspaces*

  $V = \mathbb{F}^n$, $M \in \mathrm{Mat}_n(\mathbb{F})$ 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 $\mathcal{B} = (M^i)_{i\in\mathbb{N}}$.

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

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

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

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

$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \ldots$

$a_{i+2} = 0 \quad \forall i \geq 0$

Examples

- *Krylov subspaces*

  $V = \mathbb{F}^n$, $M \in \mathrm{Mat}_n(\mathbb{F})$ 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 $\mathcal{B} = (M^i)_{i \in \mathbb{N}}$.

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

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

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

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

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

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

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

$$\mathcal{A} = (a_i)_{i \in \mathbb{N}}$$

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

$$f(x) = f_0 + f_1 x + \cdots + f_d x^d \longleftrightarrow \mathrm{rev}_d(f) = x^d f(x^{-1})$$
$$= f_0 x^d + f_1 x^{d-1} + \cdots + f_d$$

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 $\mathcal{A} = (a_i)_{i \in \mathbb{N}}$
- The following lemma gives us equivalent ways of describing characteristic polynomials

Lemma (Description of Characteristic Polynomials)

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

1. $f \in Ann(\mathcal{A})$ — *f is characteristic polynomial*
2. *$r \cdot h$ is a polynomial of degree $< d$*

$g = h \cdot x$

Moreover, if $f(x)$ is the minimal polynomial of $\mathcal{A}$, then

$$d = \max\{1 + \deg(g), \deg r\} \quad \textit{and} \quad \gcd(g, r) = 1$$

Characterizing Minimal Polynomial

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

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

polynomial of degree $< d$

$$f(x) = f_d x^d + f_{d-1} x^{d-1} + \cdots + f_0$$

$$r(x) = f_d + f_{d-1} x + \cdots + f_0 x^d$$

$$[h \cdot r]_{d+k} = \left[(a_0 + a_1 x + \cdots + \quad)(f_d + f_{d-1} x + \cdots + f_0 x^d) \right]_{d+k}$$

$$= \boxed{f_d \cdot a_{d+k} + f_{d-1} \cdot a_{d+k-1} + f_{d-2} a_{d+k-2} + \cdots + f_0 a_k}$$

f characteristic $\Rightarrow$ $f_d a_{d+k} + \cdots + f_0 a_k = 0 \quad \forall k \geq 0$

$\Rightarrow [h \cdot r]_{d+k} = 0 \quad \forall k \geq 0$

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 $h(x) \cdot r(x)$

$k \geq 0$

$$0 = [h \cdot r]_{d+k} = f_d a_{d+k} + f_{d-1} a_{d+k-1} + \cdots + f_0 a_k$$

$$\Updownarrow$$

$f(x)$ 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

$\deg(g) < \deg(f) = d$

$\deg(r) = d$ $\quad r(x) = x^d \cdot f(1/x)$

$\deg(r) < \deg(f)$ iff $x \mid f$ $(f_0 = 0)$

$\boxed{p = f/x}$ characteristic polynomial

- 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

$h \cdot r = g$

$h \cdot \underbrace{\left(\frac{r}{q}\right)}_{\hat{r}} = \underbrace{\left(\frac{g}{q}\right)}_{\tilde{g}}$

$\boxed{h \cdot \hat{r} = \hat{g}}$

$\ell = d - e$

$\hat{r}(x) = \underbrace{r_0}_{\neq 0} + \cdots + r_\ell x^\ell$

$\hat{g}(x) = g_0 + \cdots$

$\deg(\hat{g}) < \deg(\mathrm{rev}(\hat{r}))$

- 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 $\boxed{rev_{d-e}(r/q)}$ is also a characteristic polynomial, since

$$rev_{d-e}(rev_{d-e}(r/q)) = r/q$$

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 $rh = g$.

[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:

$$h \equiv \frac{g}{r} \mod x^{2n}, \quad \underbrace{x \nmid r}_{\substack{r_0 \neq 0 \\ (r_0 = 1)}} \quad \deg(g) < n, \quad \deg(r) \leq n, \quad \gcd(r, g) = 1$$

[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:

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

- 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 $rev_n(r)$ will satisfy, so it is a characteristic polynomial!

$$a_0, a_1, a_2, \dots, a_{n-1}, \underbrace{a_n, a_{n+1}, \dots, a_{2n-1}} \quad \underline{a_{2n}}$$

---

[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 $rev(r)$ 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 $a_0, \ldots, a_{2n-1} \in \mathbb{F}$
- **Output:** the minimal polynomial for the sequence $\mathcal{A} = (a_i)_{i \in \mathbb{N}}$

Algorithm

$$x, g \xmapsto{EA} \gcd(x, g)$$

$$\boxed{\hat{r} = \frac{r}{\gcd} \quad \hat{g} = g/\gcd}$$

- **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 $\mathcal{A} = (a_i)_{i \in \mathbb{N}}$
- 1. Find $g, r \in \mathbb{F}[x]$ that solve the following system:

$$\overbrace{h \equiv \frac{g}{r} \mod x^{2n}, \quad \underset{r_0 = 1}{\boxed{x \nmid r}} \quad \deg(g) < n, \quad \deg(r) \le n,}\quad \gcd(r, g) = 1$$

$$\underbrace{h = a_0 + a_1 x + a_2 x^2 + \cdots + a_{2n-1} x^{2n-1}}_{\text{given}} \mod x^{2n}$$

$$\boxed{h \cdot r \equiv g}$$

linear system of equations

$$g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_{n-1} x^{n-1}$$

$$r(x) = 1 + r_1 x + r_2 x^2 + \cdots + r_n x^n$$

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 $\mathcal{A} = (a_i)_{i \in \mathbb{N}}$
-
  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 $rev_d(r)$

moreover part of minimal polynomial

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 $\mathcal{A} = (a_i)_{i \in \mathbb{N}}$
- 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 $rev_d(r)$
- 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!

References I

von zur Gathen, J. and Gerhard, J. 2013.
Modern Computer Algebra
Cambridge University Press

Chapter 12