Minimum Polynomials of Linear Transformations

Spencer De Chenne

University of Puget Sound

30 April 2014

Table of Contents

Polynomials

Given a field $\mathbb{F}$, we denote the set of all polynomials with coefficients in $\mathbb{F}$ by $\mathbb{F}[x]$.

Polynomials

Given a field $\mathbb{F}$, we denote the set of all polynomials with coefficients in $\mathbb{F}$ by $\mathbb{F}[x]$.

Eg.

- $f(x) = x^4 - \frac{5}{9}x^3 + 5 \in \mathbb{Q}[x]$
- $g(x) = \pi x^3 - ex^2 + i \in \mathbb{C}[x]$

Irreducible Polynomials

Definition

A non-constant polynomial $f(x) \in \mathbb{F}[x]$ is irreducible if there are no $g(x), h(x) \in \mathbb{F}[x]$, where the degrees of $g(x)$ and $h(x)$ are both less than the degree of $f(x)$, such that $f(x) = g(x)h(x)$.

Irreducible Polynomials

Definition

A non-constant polynomial $f(x) \in \mathbb{F}[x]$ is irreducible if there are no $g(x), h(x) \in \mathbb{F}[x]$, where the degrees of $g(x)$ and $h(x)$ are both less than the degree of $f(x)$, such that $f(x) = g(x)h(x)$.

For our purposes, think of irreducible polynomials as equivalent to prime numbers.

Irreducible examples

Consider $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$:

- $x^2 - 2$: irreducible in $\mathbb{Q}[x]$

Irreducible examples

Consider $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$:

- $x^2 - 2$: irreducible in $\mathbb{Q}[x]$
- $x^3 - 15x^2 - 45x + 21$: irreducible in $\mathbb{Q}[x]$

Irreducible examples

Consider $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$:

- $x^2 - 2$: irreducible in $\mathbb{Q}[x]$
- $x^3 - 15x^2 - 45x + 21$: irreducible in $\mathbb{Q}[x]$
- $x^2 + 1$: irreducible in $\mathbb{R}[x]$ and $\mathbb{Q}[x]$

Irreducible examples

Consider $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$:

- $x^2 - 2$: irreducible in $\mathbb{Q}[x]$
- $x^3 - 15x^2 - 45x + 21$: irreducible in $\mathbb{Q}[x]$
- $x^2 + 1$: irreducible in $\mathbb{R}[x]$ and $\mathbb{Q}[x]$

Which polynomials are irreducible in $\mathbb{C}[x]$:

Irreducible examples

Consider $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$:

- $x^2 - 2$: irreducible in $\mathbb{Q}[x]$
- $x^3 - 15x^2 - 45x + 21$: irreducible in $\mathbb{Q}[x]$
- $x^2 + 1$: irreducible in $\mathbb{R}[x]$ and $\mathbb{Q}[x]$

Which polynomials are irreducible in $\mathbb{C}[x]$: only linear factors.

Irreducible Factors

What is important about irreducible polynomials?

Irreducible Factors

What is important about irreducible polynomials?

Theorem

Let $f(x) \in \mathbb{F}[x]$ be a non-constant polynomial. Then $f(x)$ is a unique (up to order) product of irreducible factors.

Irreducible Factors

What is important about irreducible polynomials?

Theorem

Let $f(x) \in \mathbb{F}[x]$ be a non-constant polynomial. Then $f(x)$ is a unique (up to order) product of irreducible factors.

Think about this like an integer being a product of prime numbers.

Monic Polynomials

Definition

A polynomial $f(x) \in \mathbb{F}[x]$ is monic if its leading coefficient is 1.

Monic Polynomials

Definition

A polynomial $f(x) \in \mathbb{F}[x]$ is monic if its leading coefficient is 1.

Eg.

- $f(x) = x^4 + 3x^3 - 1$ is monic
- $g(x) = 2x^7 - 6x^3$ is not monic

Endomorphisms

Minimum polynomials are only used for a specific type of linear transformation: endomorphisms.

Definition

An endomorphism T is a linear transformation mapping from a vector space V onto itself (i.e. $T : V \to V$). For a vector space V, we shall denote the set of all endomorphisms of V as $\text{End}(V)$.

More Endomorphisms

Remark

Notice that for $R, S \in \operatorname{End}(V)$, their composition, $R \circ S$, is also an endomorphism. Also, for $\alpha \in \mathbb{F}$, $\alpha R \in \operatorname{End}(V)$.

More Endomorphisms

Remark

Notice that for $R, S \in \operatorname{End}(V)$, their composition, $R \circ S$, is also an endomorphism. Also, for $\alpha \in \mathbb{F}$, $\alpha R \in \operatorname{End}(V)$.

We denote the n^{th} iterate of T by

$$T^n = \underbrace{T \circ T \circ \cdots \circ T}_{\text{n times}}.$$

More Endomorphisms

Remark

Notice that for $R, S \in \text{End}(V)$, their composition, $R \circ S$, is also an endomorphism. Also, for $\alpha \in \mathbb{F}$, $\alpha R \in \text{End}(V)$.

We denote the n^{th} iterate of T by

$$T^n = \underbrace{T \circ T \circ \cdots \circ T}_{\text{n times}}.$$

From the previous two remarks, we can see that for $T \in \text{End}(V)$ and $p(x) \in \mathbb{F}[x]$, then

$$p(T) \in \text{End}(V).$$

Annihilator Polynomial

Theorem

Let V be a vector space of dimension n, $v \in V$ a non-zero vector, and T an endomorphism of V. Then there is a unique monic polynomial of minimum degree, $m_{T,v}(x)$, such that $m_{T,v}(v) = 0$. This polynomial has degree at most n.

This polynomial, $m_{T,v}(x)$, is called the T-annihilator polynomial for v.

Proof of Annihilator Polynomial

Proof Sketch

- The set $\{T^n(v), T^{n-1}(v), ..., T(v), v\}$ is a set of $n+1$ vectors in an n-dimensional vector space, and must be linearly dependent.

Proof of Annihilator Polynomial

Proof Sketch

- The set $\{T^n(v), T^{n-1}(v), ..., T(v), v\}$ is a set of $n+1$ vectors in an n-dimensional vector space, and must be linearly dependent.
- There exist scalars $a_n, ..., a_1, a_0$ such that

$$a_n T^n(v) + \cdots + a_1 T(v) + a_0 v = 0.$$

Proof of Annihilator Polynomial

Proof Sketch

- The set $\{T^n(v), T^{n-1}(v), ..., T(v), v\}$ is a set of $n+1$ vectors in an n-dimensional vector space, and must be linearly dependent.
- There exist scalars $a_n, ..., a_1, a_0$ such that

$$a_n T^n(v) + \cdots + a_1 T(v) + a_0 v = 0.$$

- Define $f(x) = a_n x^n + \cdots + a_1 x + a_0$. We can make this polynomial monic and show it satisfies the other properties of the T-annihilator polynomial of v.

Minimum Polynomial

Theorem

Let V be an n-dimensional vector space, and T and endomorphism of V. Then there exists a unique monic polynomial of minimum degree, $m_T(x)$, such that $m_T(v) = 0$ for every $v \in V$. This polynomial has degree at most n.

We call this polynomial, $m_T(x)$, the minimum polynomial of T.

Characteristic Polynomial

Definition

For an endomorphism T of V with matrix representation $[T]_B$ relative to basis B, the characteristic polynomial of T, $c_T(x)$, is the polynomial

$$c_T(x) = \det\left(xI - [T]_B\right).$$

Characteristic Polynomial

Definition

For an endomorphism T of V with matrix representation $[T]_B$ relative to basis B, the characteristic polynomial of T, $c_T(x)$, is the polynomial

$$c_T(x) = \det\left(xI - [T]_B\right).$$

Theorem

If A and B be similar matrices, then the characteristic polynomials of A and B, $c_A(x)$ and $c_B(x)$, are equal.

We can see that the characteristic polynomial of T is a well-defined polynomial.

Companion Matrix

Definition

Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a monic polynomial of degree $n \geq 1$. Then the companion matrix of $f(x)$, $C(f(x))$, is the $n \times n$ matrix

$$C(f(x)) = \begin{bmatrix} -a_{n-1} & 1 & 0 & \cdots & 0 \\ -a_{n-2} & 0 & 1 & \cdots & 0 \\ & & \vdots & \ddots & \\ -a_1 & 0 & 0 & \cdots & 1 \\ -a_0 & 0 & 0 & \cdots & 0 \end{bmatrix},$$

where the 1's are located on the super-diagonal.

Applications of Companion Matrix

Why do we care about the Companion Matrix?

Applications of Companion Matrix

Why do we care about the Companion Matrix?

Theorem

Let $f(x)$ be a polynomial, and $A = C(f(x))$ its companion matrix. Then $c_A(x) = \det(xI - A) = f(x)$. Further, $m_A(x) = f(x)$.

We can create linear transformations with eigenvalue properties we want.

Building Endomorphisms

Suppose we want a linear transformation, T, with eigenvalues $\lambda = -1, 3, 4$, and algebraic multiplicities $\alpha(-1) = \alpha(3) = \alpha(4) = 1$.

Building Endomorphisms

Suppose we want a linear transformation, T, with eigenvalues $\lambda = -1, 3, 4$, and algebraic multiplicities $\alpha(-1) = \alpha(3) = \alpha(4) = 1$.

- First build $c_T(x)$:

$$c_T(x) = (x+1)(x-3)(x-4) = x^3 - 6x^2 + 5x + 12$$

Building Endomorphisms

Suppose we want a linear transformation, T, with eigenvalues $\lambda = -1, 3, 4$, and algebraic multiplicities $\alpha(-1) = \alpha(3) = \alpha(4) = 1$.

- First build $c_T(x)$:

$$c_T(x) = (x+1)(x-3)(x-4) = x^3 - 6x^2 + 5x + 12$$

- Then build $C(c_T(x))$:

$$C(c_T(x)) = \begin{pmatrix} 6 & 1 & 0 \\ -5 & 0 & 1 \\ -12 & 0 & 0 \end{pmatrix}$$

- Boom.

Another Example

Let's do a larger example: $c_T(x) = (x^2 + 2)^2(x^4 + 1)$.

Another Example

Let's do a larger example: $c_T(x) = (x^2+2)^2(x^4+1)$. Then

$$C(c_T(x)) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ -5 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ -4 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

This linear transformation preserves eigenvalues and algebraic multiplicities of eigenvalues.

Relationship between $m_T(x)$ and $c_T(x)$

So far, our examples have shown that $m_T(x) = c_T(x)$. This is not true in general.

Consider

$$T = \begin{pmatrix} 3 & 3 & 3 \\ 4 & 4 & 4 \\ 5 & 5 & 5 \end{pmatrix}.$$

Relationship between $m_T(x)$ and $c_T(x)$

So far, our examples have shown that $m_T(x) = c_T(x)$. This is not true in general.

Consider

$$T = \begin{pmatrix} 3 & 3 & 3 \\ 4 & 4 & 4 \\ 5 & 5 & 5 \end{pmatrix}.$$

Then $c_T(x) = x^2(x - 12)$. However, we can compute that

$$\ker\left(T(T - 12I)\right) = \mathbb{Q}^3.$$

Relationship between $m_T(x)$ and $c_T(x)$

So far, our examples have shown that $m_T(x) = c_T(x)$. This is not true in general.

Consider

$$T = \begin{pmatrix} 3 & 3 & 3 \\ 4 & 4 & 4 \\ 5 & 5 & 5 \end{pmatrix}.$$

Then $c_T(x) = x^2(x-12)$. However, we can compute that

$$\ker(T(T-12I)) = \mathbb{Q}^3.$$

We will see that this implies

$$m_T(x) = x(x-12),$$

and $m_T(x) \neq c_T(x)$.

Relationship between $m_T(x)$ and $c_T(x)$

Theorem

Let V be a finite-dimensional vector space, and T and endomorphism of V. Let $m_T(x)$ and $c_T(x)$ be the minimum and characteristic polynomials of T, respectively. Then $m_T(x)$ divides $c_T(x)$, and every irreducible factor of $c_T(x)$ is also an irreducible factor of $m_T(x)$.

Kernels of Polynomials

Theorem

Let V be an n-dimensional vector space, T and endomorphism of V, and $p(x) \in \mathbb{F}[x]$. Then,

$$\ker(p(T)) = \{v \in V : p(T)(v) = 0\}$$

is a T-invariant subspace of V.

Direct Sums via Minimum Polynomials

For a special case of an endomorphism, we can use the minimum polynomial to write V as the direct sum of invariant subspaces.

Theorem

Let V be a vector space, and T an endomorphism of V. Suppose $m_T(x)$ factors into pairwise relatively prime polynomials $m_T(x) = p_1(x)p_2(x)\cdots p_k(x)$. For each i, let $W_i = \ker(p_i(T))$. Then each W_i is T-invariant, and

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_k.$$

Last Example

Recall

$$A = \begin{pmatrix} 6 & 1 & 0 \\ -5 & 0 & 1 \\ -12 & 0 & 0 \end{pmatrix}.$$

Last Example

Recall

$$A = \begin{pmatrix} 6 & 1 & 0 \\ -5 & 0 & 1 \\ -12 & 0 & 0 \end{pmatrix}.$$

Then, $m_A(x) = (x+1)(x-3)(x-4)$.

Last Example

Recall

$$A = \begin{pmatrix} 6 & 1 & 0 \\ -5 & 0 & 1 \\ -12 & 0 & 0 \end{pmatrix}.$$

Then, $m_A(x) = (x+1)(x-3)(x-4)$.

We know

$$\begin{aligned} \mathbb{Q}^3 &= \ker(T+1) \oplus \ker(T-3) \oplus \ker(T-4) \\ &= \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 9 \\ 3 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 16 \\ 4 \\ 1 \end{pmatrix}. \end{aligned}$$

Bibliography

[1] Weintraub, Steven H. *A Guide to Advanced Linear Algebra.* United States of America: The Mathematical Association of America, 2011.

[2] Curtis, Morton L. *Abstract Linear Algebra.* New York: Springer-Verlag, 1990.