Math 5327
Spring 2018

The Cayley-Hamilton Theorem and Minimal Polynomials

Here are some notes on the Cayley-Hamilton Theorem, with a few extras thrown in. I will start with a proof of the Cayley-Hamilton theorem, that the characteristic polynomial is an annihilating polynomial for its $n \times n$ matrix A, along with a 3×3 example of the various aspects of the proof. In class, I only used a 2×2 example, which seems a little too simple.

The proof starts this way: given a matrix, A, we consider the formula

$$(xI - A)\mathrm{adj}(xI - A) = \det(xI - A)I = c_A(x)I.$$

It would be nice to just plug A into this equation for x, and say that $A - A = 0$, so the result follows. This does not work because $\mathrm{adj}(xI - A)$ has entries which are polynomials in x so we would be dealing with a matrix where some of its entries are scalars and others are matrices. For example, if

$$A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}, \quad \text{then} \quad \mathrm{adj}(xI - A) = \begin{pmatrix} x^2 - 4x + 3 & x - 1 & x - 1 \\ x - 1 & x^2 - 4x + 3 & x - 1 \\ x - 1 & x - 1 & x^2 - 4x + 3 \end{pmatrix}.$$

Also,

$$(xI - A)\mathrm{adj}(xI - A) = (x^3 - 6x^2 + 9x - 4)I.$$

What we do is write $\mathrm{adj}(xI - A)$ as a polynomial with matrix coefficients. In this case,

$$\mathrm{adj}(xI - A) = x^2 I + x\begin{pmatrix} -4 & 1 & 1 \\ 1 & -4 & 1 \\ 1 & 1 & -4 \end{pmatrix} + \begin{pmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix}.$$

More generally,

$$\mathrm{adj}(xI - A) = x^{n-1}B_{n-1} + x^{n-2}B_{n-2} + \cdots + xB_1 + B_0$$

for some collection of matrices. At this point, we have

$$\left(xI - \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}\right)\left(x^2 I + x\begin{pmatrix} -4 & 1 & 1 \\ 1 & -4 & 1 \\ 1 & 1 & -4 \end{pmatrix} + \begin{pmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix}\right) = (x^3 - 6x^2 + 9x - 4)I,$$

and it is legal to replace x by a matrix. This does not mean it is valid to do so, just that the expressions can make mathematical sense at this point. For example, if we were to replace x by, say, $C = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, then on the left hand side of the expression above we have

$$\left(\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} - \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}\right)\left(0I + \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} -4 & 1 & 1 \\ 1 & -4 & 1 \\ 1 & 1 & -4 \end{pmatrix} + \begin{pmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix}\right)$$

$$= \begin{pmatrix} -2 & -1 & 0 \\ -1 & -2 & -1 \\ -1 & -1 & -2 \end{pmatrix}\begin{pmatrix} 4 & 0 & -5 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix} = \begin{pmatrix} -7 & -3 & 11 \\ -1 & -5 & 4 \\ -1 & -1 & 0 \end{pmatrix}.$$

On the other hand,

$$(x^3-6x^2+9x-4)I = 0+0+9\begin{pmatrix}0&0&1\\0&0&0\\0&0&0\end{pmatrix} - 4\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} = \begin{pmatrix}-4&0&9\\0&-4&0\\0&0&-4\end{pmatrix},$$

a very different answer.

Thus,

$$(xI-A)(x^{n-1}B_{n-1}+x^{n-2}B_{n-2}+\cdots+xB_1+B_0) = c_A(x)I$$

is correct for scalars x but not for matrices. Now if x is a scalar, we can multiply the left hand side out, and collect powers of x to get

$$x^nI + x^{n-1}(B_{n-2}-AB_{n-1}) + \cdots + x(B_0-AB_1) - AB_0.$$

If we denote $c_A(x)$ by $x^n + a_{n-1}x^{n-1}+\cdots+xa_1+a_0$ then

$$\begin{aligned} x^nB_{n-1} + x^{n-1}(B_{n-2}-AB_{n-1}) + \cdots + x(B_0-AB_1) - AB_0 \\ = x^nI + a_{n-1}x^{n-1}I+\cdots+xa_1I+a_0I. \end{aligned} \tag{1}$$

Two polynomials are equal if and only if they have the same coefficients, and this is true even if those coefficients are matrices. Consequently, $B_{n-1}=I,\ B_{n-2}-AB_{n-1}=a_{n-1}I,\ \ldots,\ B_0-aB_1=a_1I,\ -AB_0=a_0I$. In fact, for our running example, we see that $B_2=I,\ B_1-AB_2=-6I,\ B_0-AB_1=\begin{pmatrix}3&-1&-1\\-1&3&-1\\-1&-1&3\end{pmatrix}-\begin{pmatrix}2&1&1\\1&2&1\\1&1&2\end{pmatrix}\begin{pmatrix}-4&1&1\\1&-4&1\\1&1&-4\end{pmatrix}=9I$ and $-AB_0=-4I$. At this point, it is possible to replace x by any 3×3 matrix, and everything will work. The problem is that for general matrices x, it need not be the case that

$$\begin{aligned}&(xI-A)(x^{n-1}B_{n-1}+x^{n-2}B_{n-2}+\cdots+xB_1+B_0)\\ &\qquad = x^nB_{n-1}+x^{n-1}(B_{n-2}-AB_{n-1})+\cdots+x(B_0-AB_1)-AB_0.\end{aligned}$$

That is, this equation is true for all scalars x but not all matrices. What does it take to make it true for matrices? We must pay attention to order in matrix multiplication. A careful multiplication shows

$$\begin{aligned}&(xI-A)(x^{n-1}B_{n-1}+x^{n-2}B_{n-2}+\cdots+xB_1+B_0)\\ &\qquad = x^nB_{n-1}+(x^{n-1}B_{n-2}-Ax^{n-1}B_{n-1})+\cdots+(xB_0-AxB_1)-AB_0.\end{aligned}$$

To make

$$x^nB_{n-1}+(x^{n-1}B_{n-2}-Ax^{n-1}B_{n-1})+\cdots+(xB_0-AxB_1)-AB_0$$

look like

$$x^nB_{n-1}+x^{n-1}(B_{n-2}-AB_{n-1})+\cdots+x(B_0-AB_1)-AB_0$$

we need x to be able to commute with all powers of A. This was the problem with the matrix C we plugged in for x, that $AC \neq CA$. But A obviously commutes with all powers of A so it is legal to replace x with A. When we do, we get

$$c_A(A) = A^n B_{n-1} + A^{n-1}(B_{n-2} - AB_{n-1}) + \cdots + A(B_0 - AB_1) - AB_0,$$

and you can see by the cancellation that this will be 0. This completes the proof.

Here is an extension of the Cayley-Hamilton Theorem. It uses $\operatorname{adj}(xI - A)$ to calculate the minimal polynomial of A. Suppose that the greatest common divisor of all the entries in $\operatorname{adj}(xI-A)$ is $g(x)$. Then the minimal polynomial is $m_A(x) = \dfrac{c_A(x)}{g(x)}$. The proof is essentially the same as the proof of the Cayley-Hamilton theorem. If every entry in $\operatorname{adj}(xI - A)$ is divisible by $g(x)$ then we may factor $g(x)$ outside the matrix, and then write the remaining matrix as a polynomial in x. This would give

$$\operatorname{adj}(xI - A) = g(x)(x^m C_m + x^{m-1}C_{m-1} + \cdots + xC_1 + C_0)$$

for some matrices $C_0, \ldots, C_m$. This means

$$c_A(x)I = g(x)(xI - A)(x^m C_m + x^{m-1}C_{m-1} + \cdots + xC_1 + C_0),$$

or

$$[c_A(x)/g(x)]I = (xI - A)(x^m C_m + x^{m-1}C_{m-1} + \cdots + xC_1 + C_0).$$

We now follow the rest of the proof of the Cayley-Hamilton theorem to justify that this equation remains valid when x is replaced by A.

Next, if $f(x) = x^n C_n + \cdots + xC_1 + C_0$ is any polynomial with matrix coefficients, then if x is a variable that commutes with A we can divide by $xI - A$ to get

$$f(x) = (xI - A)q(x) + R,$$

for some polynomial $q(x)$ with matrix coefficients and some matrix R. If $f(x)$ annihilates A then $0 = f(A) = (A - A)q(A) + R$ forces $R = 0$. In particular, if $m_A(x)$ is the minimal polynomial of A then we can write $m_A(x) = (xI - A)q(x)$ for some polynomial with matrix coefficients. If $c_A(x) = m_A(x)h(x)$ then we have

$$(xI - A)\operatorname{adj}(xI - A) = c_A(x)I = m_A(x)h(x)I = (xI - A)h(x)q(x).$$

Comparing the start and the end, $\operatorname{adj}(xI-A) = h(x)q(x) = h(x)Q(x)$ where $Q(x)$ is a single matrix (not a polynomial) but with polynomial entries. This means that every entry in the adjoint of $xI - A$ must be divisible by $h(x)$, and this finishes the proof. For example, with the matrix A we have been using as an example, if you look back at the adjoint of $xI - A$ and note that $x^2 - 4x + 3 = (x-1)(x-3)$ then we see that $x - 1$ is the greatest common divisor of the entries of the adjoint. The characteristic polynomial is $x^3 - 6x^2 + 9x - 4 = (x-1)^2(x-4)$.

This means the minimal polynomial of A should be $\dfrac{(x-1)^2(x-4)}{x-1} = (x-1)(x-4)$, which is easy to check.

For another example, let $A = \begin{pmatrix} 3 & 1 & 1 & 1 \\ 1 & 3 & 1 & 1 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 1 & 3 \end{pmatrix}$. In this case, the adjoint is

$$\begin{pmatrix} (x-2)(x-3)(x-4) & (x-2)(x-4) & (x-2)^2 & (x-2)^2 \\ (x-2)(x-4) & (x-2)(x-3)(x-4) & (x-2)^2 & (x-2)^2 \\ 0 & 0 & (x-2)(x-3)(x-4) & (x-2)(x-4) \\ 0 & 0 & (x-2)(x-4) & (x-2)(x-3)(x-4) \end{pmatrix}.$$

As we can see, the gcd of the terms in the adjoint is $x-2$. You should check that the characteristic polynomial is $(x-2)^2(x-4)^2$ and that the minimal polynomial is $(x-2)(x-4)^2$.

One final note on this material. A matrix with integer entries or polynomial entries can be put into a special form, called the **Smith-Normal** form: Given A there are matrices P and Q each with determinant ± 1 for which $PAQ = \begin{pmatrix} c_1 & & & \\ & c_2 & & \\ & & \ddots & \\ & & & c_n \end{pmatrix}$, a diagonal matrix. In this matrix, each entry should divide subsequent entries. That is, c_n is divisible by c_{n-1} is divisible by c_{n-2}, and so on. Moreover, $\det(A) = \pm c_1 c_2 \cdots c_n$. If we find the Smith-Normal form for $xI - A$ then we can make all the $c's$ be monic polynomials, their product will be the characteristic polynomial, and c_n will be the minimal polynomial. Let's show this on the matrix A above. We do row and column operations on $xI - A$, but if we multiply or divide a row by anything other than 1 or -1 we must do the reverse later. The method is to write the greatest common divisor of all the entries as a combination of the entries, use row/column operations to produce that gcd, interchange rows and columns to put that element in the (1, 1) position, and use it to get rid of everything in its row and column. Then work on the $(n-1) \times (n-1)$ submatrix that's left, etc. In our case, the calculations look like this:

$$xI - A = \begin{pmatrix} x-3 & -1 & -1 & -1 \\ -1 & x-3 & -1 & -1 \\ 0 & 0 & x-3 & -1 \\ 0 & 0 & -1 & x-3 \end{pmatrix} \Rightarrow \begin{pmatrix} -1 & x-3 & -1 & -1 \\ x-3 & -1 & -1 & -1 \\ 0 & 0 & x-3 & -1 \\ 0 & 0 & -1 & x-3 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} -1 & x-3 & -1 & -1 \\ 0 & x^2-6x+8 & -x+2 & -x+2 \\ 0 & 0 & x-3 & -1 \\ 0 & 0 & -1 & x-3 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x^2-6x+8 & -x+2 & -x+2 \\ 0 & 0 & x-3 & -1 \\ 0 & 0 & -1 & x-3 \end{pmatrix}.$$

In the lower right 3×3 submatrix, the greatest common divisor of the entries is still 1. We could bring the (4, 3) entry to the (2, 2) entry by row/column operations. Doing this and continue the reduction:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x^2-6x+8 & -x+2 & -x+2 \\ 0 & 0 & x-3 & -1 \\ 0 & 0 & -1 & x-3 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & x-3 \\ 0 & 0 & x-3 & -1 \\ 0 & x^2-6x+8 & -x+2 & -x+2 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & x-3 \\ 0 & x-3 & 0 & -1 \\ 0 & -x+2 & x^2-6x+8 & -x+2 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & x-3 \\ 0 & 0 & 0 & x^2-6x+8 \\ 0 & 0 & x^2-6x+8 & -(x^2-4x+4) \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & x^2-6x+8 \\ 0 & 0 & x^2-6x+8 & -(x^2-4x+4) \end{pmatrix}.$$

Now things get more complicated. Each of the for lower right entries is divisible by $x-2$, since $x^2-6x+8=(x-2)(x-4)$ and $x^2-4x+4=(x-2)^2$. If we interchange the third and fourth rows, and then the third and fourth columns, and then add the bottom row from to third, we get

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -x^2+4x-4 & x^2-6x+8 \\ 0 & 0 & x^2-6x+8 & 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -2x+4 & x^2-6x+8 \\ 0 & 0 & x^2-6x+8 & 0 \end{pmatrix}$$

Fractions arise when using the (3, 3) entry: We multiply the third row by $\frac{1}{2}(x-4)$ and add to the bottom:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -2x+4 & x^2-6x+8 \\ 0 & 0 & 0 & \frac{1}{2}(x-4)(x^2-6x+8) \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -2x+4 & 0 \\ 0 & 0 & 0 & \frac{1}{2}(x-4)(x^2-6x+8) \end{pmatrix}.$$

Finally, we make the diagonal polynomials monic by dividing the (3, 3) entry by -2, multiplying the (4, 4) entry by 2. Factoring, we have the Smith-Normal form:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x-2 & 0 \\ 0 & 0 & 0 & (x-2)(x-4)^2 \end{pmatrix}.$$

Thus, the minimal polynomial is $(x-2)(x-4)^2$ and the characteristic polynomial polynomial is the product of the diagonals: $(x-2)^2(x-4)^2$.