What is the Cayley–Hamilton Theorem?

Nicholas J. Higham[*]

November 3, 2020

The Cayley–Hamilton Theorem says that a square matrix A satisfies its characteristic equation, that is $p(A) = 0$ where $p(t) = \det(tI - A)$ is the characteristic polynomial. This statement is not simply the substitution "$p(A) = \det(A - A) = 0$", which is not valid since t must remain a scalar inside the det term. Rather, for an $n \times n$ A, the characteristic polynomial has the form

$$p(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$$

and the Cayley–Hamilton theorem says that

$$p(A) = A^n + a_{n-1}A^{n-1} + \cdots + a_1 A + a_0 I = 0.$$

Various proofs of the theorem are available, of which we give two. The first is the most natural for anyone familiar with the Jordan canonical form. The second is more elementary but less obvious.

First proof.

Consider a 4×4 Jordan block with eigenvalue λ:

$$J = \begin{bmatrix} \lambda & 1 & 0 & 0 \\ & \lambda & 1 & 0 \\ & & \lambda & 1 \\ & & & \lambda \end{bmatrix}.$$

We have

$$J - \lambda I = \begin{bmatrix} 0 & 1 & 0 & 0 \\ & 0 & 1 & 0 \\ & & 0 & 1 \\ & & & 0 \end{bmatrix}, \quad (J - \lambda I)^2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ & 0 & 0 & 1 \\ & & 0 & 0 \\ & & & 0 \end{bmatrix}, \quad (J - \lambda I)^3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ & 0 & 0 & 0 \\ & & 0 & 0 \\ & & & 0 \end{bmatrix},$$

and then $(J - \lambda I)^4 = 0$. In general, for an $n \times n$ Jordan block J with eigenvalue λ, $(J - \lambda I)^k$ is zero apart from a kth superdiagonal of ones for $k \le n-1$, and $(J - \lambda I)^n = 0$.

Let A have the Jordan canonical form $A = ZJZ^{-1}$, where $J = \text{diag}(J_1, \ldots, J_k)$ and each J_i is an $m_i \times m_i$ Jordan block with eigenvalue λ_i. The characteristic polynomial of

---
[*]Department of Mathematics, University of Manchester, Manchester, M13 9PL, UK (nick.higham@manchester.ac.uk).

A can be factorized as $p(t) = (t - \lambda_1)^{m_1}(t - \lambda_2)^{m_2} \ldots (t - \lambda_k)^{m_k}$. Note that $A^i = ZJ^iZ^{-1}$ for all i, and hence $q(A) = Zq(J)Z^{-1}$ for any polynomial q. Then

$$Z^{-1}p(A)Z = p(J) = \mathrm{diag}\big(p(J_1), p(J_2), \ldots, p(J_k)\big),$$

and $p(J_i)$ is zero because it contains a factor $(J_i - \lambda_i I)^{m_i}$ and this factor is zero, as noted above. Hence $Z^{-1}p(A)Z = 0$ and therefore $p(A) = 0$.

Second Proof

Recall that the adjugate $\mathrm{adj}(B)$ of an $n \times n$ matrix B is the transposed matrix of cofactors, where a cofactor is a signed sum of products of $n - 1$ entries of B, and that $B\,\mathrm{adj}(B) = \det(B)I$. With $B = tI - A$, each entry of $\mathrm{adj}(B)$ is a polynomial of degree $n - 1$ in t, so $B^{-1} = \mathrm{adj}(B)/\det(B)$ can be written

$$(tI - A)^{-1} = \frac{\mathrm{adj}(tI - A)}{\det(tI - A)} = \frac{t^{n-1}C_{n-1} + \cdots + tC_1 + C_0}{p(t)},$$

for some matrices C_{n-1}, ..., C_0 not depending on t. Rearranging, we obtain

$$(tI - A)\big(t^{n-1}C_{n-1} + \cdots + tC_1 + C_0\big) = p(t)I,$$

and equating coefficients of t^n, ..., t^0 gives

$$C_{n-1} = I,$$
$$C_{n-2} - AC_{n-1} = a_{n-1}I,$$
$$\vdots$$
$$C_0 - AC_1 = a_1 I,$$
$$-AC_0 = a_0 I.$$

Premultiplying the first equation by A^n, the second by A^{n-1}, and so on, and adding, gives

$$0 = A^n + a_{n-1}A^{n-1} + \cdots + a_1 A + a_0 I = p(A),$$

as required. This proof is by Buchheim (1884).

Applications and Generalizations

A common use of the Cayley–Hamilton theorem is to show that A^{-1} is expressible as a linear combination of I, A, ..., A^{n-1}. Indeed for a nonsingular A, $p(A) = 0$ implies that

$$A^{-1} = -\frac{1}{a_0}\big(A^{n-1} + a_{n-1}A^{n-2} + \cdots + a_1 I\big),$$

since $a_0 = \det(A) \neq 0$.

Similarly, A^k for any $k \geq n$ can be expressed as a linear combination of I, A, ..., A^{n-1}. An interesting implication is that any matrix power series is actually a polynomial in the matrix. Thus the matrix exponential $\mathrm{e}^A = I + A + A^2/2! + \cdots$ can be written $\mathrm{e}^A = c_{n-1}A^{n-1} + \cdots + C_1 A + c_0 I$ for some scalars c_{n-1}, ..., c_0. However, the c_i depend

on A, which reduces the usefulness of the polynomial representation. A rare example of an explicit expression of this form is Rodrigues's formula for the exponential of a skew-symmetric matrix $A \in \mathbb{R}^{3 \times 3}$:

$$\mathrm{e}^A = I + \frac{\sin \theta}{\theta} A + \frac{1 - \cos \theta}{\theta^2} A^2,$$

where $\theta = \sqrt{\|A\|_F^2 / 2}$.

Cayley used the Cayley–Hamilton theorem to find square roots of a 2×2 matrix. If $X^2 = A$ then applying the theorem to X gives $X^2 - \mathrm{trace}(X)X + \det(X)I = 0$, or

$$A - \mathrm{trace}(X)X + \det(X)I = 0, \qquad (*)$$

which gives

$$X = \frac{A + \det(X)I}{\mathrm{trace}(X)}.$$

Now $\det(X) = \sqrt{\det(A)}$ and taking the trace in $(*)$ gives an equation for $\mathrm{trace}(X)$, leading to

$$X = \frac{A + \sqrt{\det(A)}\, I}{\sqrt{\mathrm{trace}(A) + 2\sqrt{\det(A)}}}.$$

With appropriate choices of signs for the square roots this formula gives all four square roots of A when A has distinct eigenvalues, but otherwise the formula can break down.

Expressions obtained from the Cayley–Hamilton theorem are of little practical use for general matrices, because algorithms that compute the coefficients a_i of the characteristic polynomial are typically numerically unstable.

The Cayley–Hamilton theorem has been generalized in various directions. The theorem can be interpreted as saying that the powers A^i for all nonnegative i generate a vector space of dimension at most n. Gerstenhaber (1961) proved that if A and B are two commuting $n \times n$ matrices then the matrices $A^i B^j$, for all nonnegative i and j, generate a vector space of dimension at most n. It is conjectured that this result extends to three matrices.

Historical Note

The Cayley–Hamilton theorem appears in the 1858 memoir in which Cayley introduced matrix algebra. Cayley gave a proof for $n = 2$ and stated that he had verified the result for $n = 3$, adding "I have not thought it necessary to undertake the labour of a formal proof of the theorem in the general case of a matrix of any degree." Hamilton had proved the result for quaternions in 1853. Cayley actually discovered a more general version of the Cayley–Hamilton theorem, which appears in an 1857 letter to Sylvester but not in any of his published work: if the square matrices A and B commute and $f(x, y) = \det(xA - yB)$ then $f(B, A) = 0$.

References

- Arthur Buchheim, Mathematical Notes, Messenger Math. 13, 62–66, 1884.

- Arthur Cayley, A Memoir on the Theory of Matrices, Philos. Trans. Roy. Soc. London 148, 17–37, 1858.
- Tony Crilly, Cayley's Anticipation of a Generalised Cayley–Hamilton Theorem, Historia Mathematica 5, 211–219, 1978.

Related Blog Posts

- What Is the Adjugate of a Matrix? (2020)
- What Is the Gerstenhaber Problem? (2020)
- What Is the Matrix Exponential? (2020)
- What Is the Square Root of a Matrix? (2020)

This article is part of the "What Is" series, available from `https://nhigham.com/category/what-is` and in PDF form from the GitHub repository `https://github.com/higham/what-is`.