Some Linear Algebra for MAN460: The Cayley Hamilton Theorem and Invariant Subspaces

Most of the material is taken from "Ordinära Differentialekvationer" by Andersson and Böiers

The Cayley Hamilton Theorem

This theorem says essentially that "A matrix satisfies its own characteristic equation". More precisely:

Theorem 1 *Let A be a square n by n- matrix, and let $p_A(\lambda)$ be its characteristic polynomial, i.e. $p_A(\lambda) = \det(\lambda I - A)$. Then $p_A(A) = 0$.*

Proof: If λ is not an eigenvalue to A, then $\lambda I - A$ is invertible, and $(\lambda I - A)(\lambda I - A)^{-1} = I$. This is well defined except for at the isolated eigenvalues of A, and so by a continuous extention, it can be considered to hold for all λ.
Now recall Cramer's rule for computing the inverse of a matrix:

$$B^{-1} = \frac{1}{\det B}\begin{pmatrix} \tilde{b}_{11} & \tilde{b}_{12} & \cdots & \tilde{b}_{1n} \\ \tilde{b}_{21} & \tilde{b}_{22} & \cdots & \tilde{b}_{2n} \\ . & . & \cdots & . \\ . & . & \cdots & . \\ \tilde{b}_{n1} & \tilde{b}_{n2} & \cdots & \tilde{b}_{nn} \end{pmatrix},$$

where the $\tilde{b}_{jk}$ are the sub determinants of B.
Using this formula for $(\lambda I - A)^{-1}$ we find

$$(\lambda I - A)^{-1} = \frac{1}{p_A(\lambda)}\begin{pmatrix} p_{11}(\lambda) & p_{12}(\lambda) & \cdots & p_{1n}(\lambda) \\ p_{21}(\lambda) & p_{22}(\lambda) & \cdots & p_{2n}(\lambda) \\ . & . & \cdots & . \\ . & . & \cdots & . \\ p_{n1}(\lambda) & p_{n2}(\lambda) & \cdots & p_{nn}(\lambda) \end{pmatrix},$$

where all $p_{jk}(\lambda)$ are polynomials of degree at most $n-1$. This means that we can write

$$p_A(\lambda)(\lambda I - A)^{-1} = \lambda^{n-1}B_{n-1} + \lambda^{n-2}B_{n-2} + \cdots + \lambda B_1 + B_0\,,$$

where the B_j's are constant n by n matrices. Hence

$$\begin{aligned} p_A(\lambda)I &= (\lambda I - A)\left(\lambda^{n-1}B_{n-1} + \lambda^{n-2}B_{n-2} + \cdots + \lambda B_1 + B_0\right) \\ &= \lambda^n B_{n-1} + \lambda^{n-1}B_{n-2} + \cdots + \lambda^2 B_1 + \lambda B_0 \\ &\qquad -\lambda^{n-1}AB_{n-1} - \lambda^{n-2}AB_{n-2} - \cdots - \lambda AB_1 - AB_0\,. \end{aligned}$$

This can only be true if the matrices corresponding to each power of λ is an identity matrix: If $p_A(\lambda) = \lambda^n + c_{n-1}\lambda^{n-1} + \cdots + c_1\lambda + c_0$, then

$$B_{n-1} = I, \quad B_{n-2} - AB_{n-1} = c_{n-1}I \quad \ldots \quad B_0 - AB_1 = c_1 I, \quad AB_0 = c_0 I\,.$$

We can now compute $p_A(A)$:

$$\begin{aligned} p_A(A) &= A^n + c_{n-1}A^{n-1} + \cdots + c_1 A + c_0 I \\ &= A^n B_{n-1} + A^{n-1}(B_{n-2} - AB_{n-1}) + \cdots + A(B_0 - AB_1) - AB_0 \\ &= 0\,, \end{aligned}$$

which follows by combining terms with the same power of A. □

Note that this theorem shows that it is never necessary to compute A to the power higher than $n-1$:

$$\begin{aligned} A^n &= -c_{n-1}A^{n-1} - c_{n-2}A^{n-2} - \cdots - c_1 A - c_0 I\,, \\ A^{n+1} &= -c_{n-1}A^n - c_{n-2}A^{n-1} - \cdots - c_1 A^2 - c_0 A \\ &= (c_{n-1}^2 - c_{n-2})A^{n-1} + (c_{n-1}c_{n-2} - c_{n-3})A^{n-2} + \cdots \\ &\qquad + (c_{n-1}c_1 - c_0)A + c_{n-1}c_0 I\,. \end{aligned}$$

This may be very advantageous from a computatinal point of view, because it is easy to find a recursive formula for the coefficients to $A^0 \ldots A^{n-1}$, and this is very much faster than to directly compute high powers of the matrix A.
In fact, there is a general procedure for computing $f(A)$ when f is an entire function (i.e. analytic in the plane). We begin by a very general result on analytic functions. A similar result holds for C^∞-functions, but then it is much harder to prove.

Lemma 1 *Let f be an anlytic function and p a polynomial of degree (exactly) n. Then there is an analytic function g and a polynomial of degree at most $n-1$ so that*

$$f(z) = g(z)p(z) + q(z)$$

Proof: We prove this by induction of n. Assume than that $p(z) = z - c$, a first degree polynomial. If $c = 0$, then clearly

$$f(z) = \sum_{k=0}^{\infty} a_k z^k = z\sum_{k=1}^{\infty} a_k z^{k-1} + a_0\,,$$

and so the lemma holds with $q(z) = a_0$, and $g(z) = \sum_{k=0}^{\infty} a_{k+1} z^k$. For a general c, we set $w = z - c$, and see that setting $F(w) = f(w + c)$, we can use the calculation for $c = 0$ to show that

$$F(w) = G(w)w + \tilde{a}_0\,,$$

which then is the same as $f(z) = G(z-c)(z-c) + \tilde{a}_0$.
Hence the lemma is true for $n = 1$. Assume now that it is true for $n = k-1$ for some $k > 1$. Any k-th degree polynomial $p(z)$ can be written

$$p(z) \quad = \quad p_1(z)(z-c)\,,$$

where $p_1(z)$ is a polynomial of degree $k-1$. By the induction hypothesis

$$f(z) \quad = \quad g_1(z)p_1(z) + q_1(z)\,,$$

where g_1 is an analytic function, and where q_1 is a polynomial of degree at most $k-2$. We also know that $g_1(z) = g(z)(z-c) + q_0$, for some analytic function g, and hence

$$\begin{aligned} f(z) &= (g(z)(z-c) + q_0)\, p_1(z) + q_1(z) \\ &= g(z)\,((z-c)p_1(z)) + q_0 p_1(z) + q_1(z) \\ &= g(z)p(z) + q(z) \end{aligned}$$

where $q(z) = q_0 p_1(z) + q_1(z)$ is a polynomial of degree at most $k-1$. Hence the lemma is also true for $n = k$, and by the induction principle, for all $n \geq 1$. □

The lemma can now be used with the characteristic polynomial of an $n \times n$ matrix: For any analytic function $f(z)$,

$$f(\lambda) \quad = \quad g(\lambda)p_A(\lambda) + q(\lambda)$$

where $q(\lambda)$ is a polynomial of degree at most $n-1$. It follows by the Cayley Hamilton theorem that

$$f(A) \quad = \quad g(A)p_A(A) + q(A) = q(A)\,,$$

and so to compute $f(A)$ it is enough to identify $q(\lambda)$.

Lemma 2 *If the polynomial $p(z)$ in Lemma 1 can be written*

$$p(z) \quad = \quad \prod_{k=1}^{m} (z - z_k)^{r_k},$$

then $q(z)$ is the uniquely determined polynomial which satisfies

$$\frac{d^j f}{dz^j}(z_k) \quad = \quad \frac{d^j f}{dz^j}(z_k)\,, \qquad\qquad j = 0, ..., (r_k - 1)$$

The proof of this lemma is an exercise.

Invariant subspaces

Let $\mathcal{V}$ be an n-dimensional vectorspace and A an operator from $\mathcal{V}$ to$\mathcal{V}$. We recall that if a basis for $\mathcal{V}$ is given, then the operator can be represented by an $n \times n$-matrix.

A linear subspace $\mathcal{V}_1 \subset \mathcal{V}$ is said to be invariant under A if for all $v \in \mathcal{V}_1$, it is true that $Av \in \mathcal{V}_1$, i.e., if

$$A\mathcal{V}_1 \subset \mathcal{V}_1$$

For an operator A, we write $\mathcal{N}(A) = \{v \in \mathcal{V} \,|\, Av = 0\}$, the so-called nullspace of A. Note that the nullspace is a linear subspace of $\mathcal{V}$.

The Cayley-Hamilton theorem implies that if $A : \mathbb{R}^n \to \mathbb{R}^n$ is an operator (represented by the matrix A) $p_A(\lambda)$ is its characteristic polynomial, then

$$\mathcal{N}(p_A(A)) \quad = \quad \mathbb{R}^n$$

You should verify that the characteristic polyomial does not depend on which basis (and hence the matrix representation of A) that is chosen, so the statement above is well defined.

Theorem 2 *Assume that $p_A(\lambda) = p_1(\lambda)p_2(\lambda)$, where p_1 and p_2 are polynomials without common factors (i.e., without common zeros). Then $\mathcal{N}(p_1(A))$ and $\mathcal{N}(p_2(A))$ are invariant subspaces for A, $\mathcal{N}(p_1(A)) \cap \mathcal{N}(p_2(A)) = \{0\}$, and each vector $v \in \mathbb{R}^n$ can be written in a unique way as $v = v_1 + v_2$, where $v_i \in \mathcal{N}(p_i(A))$, or in other words,*

$$\mathbb{R}^n \quad = \quad \mathcal{N}(p_1(A)) \oplus \mathcal{N}(p_2(A))$$

Proof: First of all, suppose that $v \in \mathcal{N}(p_i(A)) \quad i = 1, 2$. Then

$$p_i(A)Av \quad = \quad Ap_i(A)v = 0\,,$$

which proves the invariance of the subspaces $\mathcal{N}(p_i(A))$. Next, because $p_1(\lambda)$ and $p_2(\lambda)$ dont have common factors, the Euclidean algorithm can be used to prove that there are polynomials $q_1(z)$ and $q_2(z)$ so that

$$p_1(z)q_1(z) + p_2(z)q_2(z) \quad = \quad 1\,.$$

Therefore

$$p_1(A)q_1(A) + p_2(A)q_2(A) \quad = \quad I\,,$$

and therefore every vector $v \in \mathbb{R}^n$ can be written $v = v_1 + v_2$, where

$$v_1 \,=\, p_2(A)q_2(A)v \qquad\qquad v_2 \,=\, p_1(A)q_1(A)v\,,$$

and it follows that

$$p_1(A)v_1 \quad = \quad p_1(A)p_2(A)q_2(A)v \,=\, p_A(A)q_2(A)v \,=\, 0$$

so that $v_1 \in \mathcal{N}(p_1(A))$, and similarly, $v_2 \in \mathcal{N}(p_2(A))$. If $v \in \mathcal{N}(p_1(A)) \cap \mathcal{N}(p_2(A))$, then

$$v \quad = \quad q_1(A)p_1(A)v + q_2(A)p_2(A)v \; = \; 0\,,$$

which proves that $\mathcal{N}(p_1(A)) \cap \mathcal{N}(p_2(A)) = \{0\}$.

Finally, if there are two such decompositions, $v = v_1 + v_2 = w_1 + w_2$, then

$$v_1 - w_1 \quad = \quad v_2 - w_2$$

so

$$v_i - w_i \in \mathcal{N}(p_1(A)) \cap \mathcal{N}(p_2(A)) = \{0\} \qquad\qquad i = 1, 2\,,$$

and therefore $v_i = w_i$. □

A consequence of this important theorem is that given any matrix A, (or operator with representation A), there is a natural decomposition of $\mathbb{R}^n$ into subspaces which are invariant with respect to A: if

$$p_A(\lambda) \quad = \quad \prod_{k=1}^{m} (\lambda - \lambda_k)^{r_k}\,,$$

where $r_1 + ... + r_m = n$, then

$$\mathbb{R}^n \quad = \quad \mathcal{N}((A - \lambda_1)^{r_1}) \oplus ... \oplus \mathcal{N}((A - \lambda_m)^{r_m})$$