A PROOF OF THE CARTAN-DIEUDONNÉ THEOREM

Jules Jacobs

December 3, 2021

The Cartan-Dieudonné theorem is fundamental theorem about the geometry of n-dimensional space: any orthogonal transformation A can be written as a sequence of at most n reflections. The proofs that I could find go by induction on n and hence have to relate maps on $n-1$ dimensional spaces to maps on n dimensional spaces. This leads to technicalities or handwaving. We'll see a slightly modified proof that stays in n dimensions by doing induction on $\dim\ker(A-I)$.

1 THE CARTAN-DIEUDONNÉ THEOREM

The theorem we want to prove is:

Theorem 1.1 (Cartan-Dieudonné). *An orthogonal transformation* $A : \mathbb{R}^n \to \mathbb{R}^n$ *can be written as a sequence of* $k \leqslant n$ *reflections in vectors* $v_1, v_2, \ldots, v_k \in \mathbb{R}^n$*:*

$$A = R_{v_1} R_{v_2} \cdots R_{v_k}$$

where $k = n - \dim\ker(A - I)$.

The space $\ker(A - I) = \{v \in \mathbb{R}^n \mid Av = v\}$ is the subspace where the transformation A is the identity. So the Cartan-Dieudonné theorem usually decomposes an orthogonal tranformation into n reflections, but we save one reflection per direction where A is the identity. We shall see that this is the minimum number: it cannot be done with even fewer reflections.

The idea of the proof is that if we have a vector u such that $Au \neq u$, then we can compose A with the refection $R_{(Au-u)}$, which sends Au back to u, in order to make A also the identity in that direction. This reflection does not disturb any of the directions where A was already the identity. We prove the Cartan-Dieudonné theorem by iterating this processes until A is the identity in all directions. We shall now investigate this in more detail.

2 THE GEOMETRY OF ORTHOGONAL TRANFORMATIONS

A linear map $A : \mathbb{R}^n \to \mathbb{R}^n$ is an orthogonal transformation if one of the following equivalent conditions holds:

1. $A^T A = I$ (or equivalently, $A^T = A^{-1}$).
2. $\langle Av, Aw\rangle = \langle v, w\rangle$ for all v, w.
3. $||Av|| = ||v||$ for all v.

Examples of orthogonal transformations are rotations and reflections.

The reflection $R_v : \mathbb{R}^n \to \mathbb{R}^n$ in a vector v is defined as follows:

Definition 2.1. $R_v \triangleq I - 2\frac{vv^T}{|v|^2}$

On $\mathbb{R}^3$ for instance, $R_{(1,0,0)}(x, y, z) = (-x, y, z)$.

A reflection R_v is the identity on a subspace of dimension $n-1$ (namely the plane orthogonal to v), and really does something on a subspace of dimension 1. Similarly, a rotation is the identity on a subspace of dimension $n-2$ and really does something on a subspace of dimension 2. Note that the phrase "really does something" must be interpreted with care: a rotation moves almost all points of $\mathbb{R}^3$; only the axis of rotation is left fixed. But still, because these are linear maps, the action can be decomposed into a plane of rotation, and the identity on the subspace orthogonal to the plane.

The subspace on which A is the identity is $\ker(A-I) = \{u \mid Au = u\}$. The subspace orthogonal to $\ker(A-I)$ on which A really does something can be characterized in two equivalent ways:

Lemma 2.1. *If A is an orthogonal transformation, then* $\ker(A-I)^{\perp} = \operatorname{im}(A-I)$.

Proof. $\ker(A-I)^{\perp} = \operatorname{im}((A-I)^{T}) = \operatorname{im}(A^{T}-I) = \operatorname{im}(A^{-1}-I) = \operatorname{im}(A-I)$. □

This space is important because its dimension determines how many reflections we need when decomposing A: for directions in which A already is the identity we don't need any reflections.

The idea behind the proof of the Cartan-Dieudonné theorem is that we can make A be the identity in more directions by composing it with reflections, and repeat this until it is the identity in all directions. This is given in the following lemma:

Lemma 2.2. *If A is an orthogonal tranformation that is the identity in k directions, then $R_v A$ is the identity in $k+1$ directions, where v is **any** nonzero vector $v \in \operatorname{im}(A-I) \setminus \{0\}$ (i.e., in the subspace where A really does something).*

Proof. Let $v \in \operatorname{im}(A-I) \setminus \{0\}$, so there is u such that $v = Au - u \neq 0$. Then (1) $R_v A$ is still the identity everywhere A is the identity (i.e., on $\ker(A-I)$), and (2) additionally $R_v A$ is also the identity on $u \notin \ker(A-I)$.

To show (1), note that R_v is the identity on all directions orthogonal to v, which by Lemma 2.1 includes everything in $\ker(A-I)$.

To show (2), we can do an explicit calculation to show $R_{(Au-u)}Au = u$, but a picture is more instructive. □

To prove Theorem 1.1, we can repeatedly apply this lemma until A is the identity in all directions, so that we have $R_{v_k} \cdots R_{v_2} R_{v_1} A = I$, which gives $A = R_{v_1} R_{v_2} \cdots R_{v_k}$.

This is also the minimum number of reflections: if A can be written as $k \leqslant n$ reflections, then there are at least $n-k$ directions where A is the identity (e.g. if A can be written as one reflection, then it is the identity in $n-1$ directions). The only directions in which $R_{v_1} R_{v_2} \cdots R_{v_k}$ is potentially not the identity is $\operatorname{span}\{v_1, v_2, \cdots, v_k\}$.