Projection*

Graeme Taylor

April 16, 2004

In Computer Science, a projection function is one of the basic building blocks of primitive recursive functions. Given a k-dimensional array, it returns the ith element, i.e., $p_i^k : \mathbb{N}^k \to \mathbb{N}$ where $p(x_1, ..., x_k) = x_i$. This is heavily used due to the way in which composition is defined for primitive recursive functions- to obtain the effect of $(g \circ f)$, i.e., $g(f(x))$ it is necessary to use projection to extract the single argument,x- $g = Cn[f, p_1^1]$. In effect the projection reduces k-dimensional space into one dimensional space.

In Linear Algebra, a projection is a linear map on a vector space V, $\pi : V \to V$, which satisfies a further constraint: $\pi^2 = \pi$; that is, $\forall v \in V$, $\pi(\pi(v)) = \pi(v)$. It follows that any higher powers of π are also equivalent to π, by repeated application of the definition of a projection. The power notation arises from the fact that composition of linear maps is equivalent to multiplication of corresponding matrices- if a matrix P represents a projection π, the product $PP = P^2$ represents $\pi \circ \pi = \pi$, so powers of P are simply P itself.

Two fairly obvious projections exist: the zero map and the identity map. This makes intuitive sense, as $0^2 = 0$ and $1^2 = 1$. In the context of maps, repeated application of the zero map is redundant once it has been applied once, and the identity map never changes the value operated on and hence may also be applied an arbitrary number of times to no effect. It turns out that all projections can be thought of as a particular combination of these two maps:

Theorem : For a vector space V and a linear map $\alpha : V \to V$; α is a projection iff there are subspaces U,W of V such that

- $V = U \oplus W$
- $\alpha : u + w \to u \ \forall u \in U, \forall w \in W$.

*First appeared on Everything2, at *http://www.everything2.com/index.pl?node_id=1532051*

Two proofs give very different insights into how this works. The first is self-contained, appealing only to the properties given or requested; whilst the second shows how a more general and hence powerful result of linear algebra, the primary decomposition theorem, can be applied to obtain an even more elegant proof.

Note first that the projections we identified earlier, the zero and identity maps, are rather degenerate cases of this theorem. For the zero map, W is V, whilst the other subspace is the trivial set $\{\mathbf{0}\}$ - Note that whilst this means that U and W have a common element, the zero vector, this is permitted by the definition of direct sum- there may be no other common vector, however. Thus any element of V is an element of W (itself) plus the zero vector from U, and gets mapped to that element of U; hence zero is yielded in every case. For the identity map, we take U to be the vector space V, and let W be $\{\mathbf{0}\}$. Now every vector is mapped to itself (the thing in U). Thus this suggests a method of construction for a general projection.

Proof 1, forward implication

Suppose we have a linear map $\alpha : V \to V$ such that $\alpha^2 = \alpha$. Take candidates for U and W as follows: $U = \text{Im } \alpha$, $W = \text{Ker } \alpha$. We claim that $V = U \oplus W$ as desired.

Let v be an arbitrary element from V. Then obviously $v = v + \alpha(v) - \alpha(v)$. Rearranging gives $v = \alpha(v) + (v - \alpha(v))$.
By definition of image, $\alpha(v) \in \text{Im } \alpha = U$. So we need to show that $(v - \alpha(v)) \in \text{Ker } a = W$ to obtain $V = U + W$.
The definition of Ker α is that it contains all elements of V such that when α is applied to them, the zero vector is obtained. So take α of $(v - \alpha(v)) := \alpha(v) - \alpha(\alpha(v))$. Since α is a projection, this becomes $\alpha(v) - \alpha(v) = \mathbf{0}$ as desired.
We have $V = U + W$. We seek a direct sum; meaning that the expression of a v from V as $u + w$ from U, W should be unique. This is equivalent to $U \cap W = \{\mathbf{0}\}$.

So consider $x \in U \cap W$. Then $x \in U = \text{Im } \alpha$, so there is a $y \in V$ such that $x = \alpha(y)$. Further, $x \in W = \text{Ker } \alpha$ so $\alpha(x) = \mathbf{0}$. Yet $\alpha(x) = \alpha(\alpha(y)) = \alpha(y)$ (by property of projection) $= x$. So $x \in U \cap W$ implies $x = \mathbf{0}$: so $U \cap W \subseteq \{\mathbf{0}\}$. $\mathbf{0}$ is in U and W, so $\mathbf{0}$ is in $U \cap W$, giving $\{\mathbf{0}\} \subseteq U \cap W$. So $U \cap W = \{\mathbf{0}\}$.

Hence $V = U \oplus W$. We desired also that if $v = u + w$, then $\alpha(v) = u$. However, $\alpha(v) = \alpha(u + w)$ which by linearity gives $\alpha(v) = \alpha(u) + \alpha(w)$. Since $u \in U = \text{Im } \alpha$, $u = \alpha(u')$ for some u' and by property of projection $\alpha(u)$ is therefore u, whilst $w \in W = \text{Ker } \alpha$ so by defintion $\alpha(w) = 0$. Hence $\alpha(v) = u + 0 = u$. We are done.

Proof 1, backward implication

Suppose that V decomposes as a direct sum; i.e., if $v \in V$ then $v = u + w$ for unique $u \in U$, $w \in W$. We define $\alpha(v) = u$, which by uniqueness is a well-defined function. It remains to show linearity and that a is a projection.

Let $v = u + w$ and $v' = u' + w'$ be elements of V. Now for scalars λ, μ from the field,

$$\begin{aligned} \alpha(v + \mu v') &= \alpha(\lambda(u + w) + \mu(u' + w')) \\ &= \alpha((\lambda u + \mu u') + (\lambda v + \mu v')) \\ &= \lambda u + \mu u' \\ &= \lambda\alpha(u) + \mu\alpha(u') \end{aligned}$$

So the definition of linearity is met. As $\alpha(\alpha(v)) = \alpha(u) = u = \alpha(v)$, we also have that this map is a projection. We are done.

Introducing some more technology we can simplify this considerably (although some of the insight into the nuts and bolts of the process is lost.)

Proof 2

We have already discussed that the decomposition works for the identity and zero maps. So consider a projection $\pi : V \to V$ which is a projection but neither of these two maps. Then we can write the definition as $\pi^2 - \pi = 0$. Hence π satisfies the polynomial $p(t) = t^2 - t$. Since this is a degree two monic polynomial, it follows that the minimal polynomial of π is at most degree two.

Now $P(t) = t(t-1)$. If the minimal polynomial has degree one rather than two, then it must be either $m(t) = t$ or $m(t) = (t-1)$, since any polynomial that is satisfied by a linear map has its minimal polynomial as a factor. But if $m(t) = t$, we have the zero map, and if $m(t) = (t-1)$, we have the identity map. We assumed that neither of these applied; so the minimal polynomial cannot be of degree one. It is hence of degree two, and in fact must be $p(t) = t(t-1)$ by uniqueness.

Now the primary decomposition theorem applies. $m_\pi(t) = p(t) = q_1(t)q_2(t)$ with $q_1 = (t-1), q_2(t) = (t)$ coprime. So $V = W_1 \oplus W_2$ where the W_i are π invariant subspaces with minimal polynomial of $\pi|_{W_i}$ given by q_i.
But then q_1 indicates that $\pi|_{W_1}$ is the identity map, whilst q_2 indicates that $\pi|_{W_2}$ is the zero map. So given $v = w_1 + w_2$, $w_i \in W_i$, $\pi(v) = \pi(w_1 + w_2) = \pi(w_1) + \pi(w_2) = id(w_1) + zero(w_2) = w_1 + 0 = w_1$. This completes the proof.