## 1. Orthogonal projections

A subset $S$ of a vector space $V$ is *convex* if for every $v, w \in S$ and every $t \in [0,1]$, the vector $tv + (1-t)w$ also belongs to $S$.

Since $tv + (1-t)w = w + t(v-w)$, $\{tv + (1-t)w : t \in [0,1]\}$ is the line segment joining the points $v$ and $w$, a set $S$ is convex when the straight line between any two points in $S$ lies entirely in $S$. For example, balls in $\mathbb{R}^2$ (or indeed in any normed space) are convex, and every subspace is convex; on the other hand, an annulus (a disc with a hole in it) is not. Our next theorem shows that interesting things happen when we combine the geometric notion of convexity with the analytic notion of closedness.

**Theorem 1.1.** *Suppose $S$ is a nonempty closed convex subset of a Hilbert space $H$. Then for every $h \in H$ there is a unique vector $k \in S$ such that*

$$\|h - k\| = d(h, S) := \inf\{\|h - l\| : l \in S\};$$

*in other words, there is exactly one point $k$ in $S$ which is closest to $h$.*

This says that if $S$ is closed and convex, the *optimisation problem*

- minimise $\|h - l\|$ subject to the constraint $l \in S$

has a unique solution. The convexity hypothesis controls the geometry of the set $S$, and is a desirable feature of optimisation problems. The closedness hypothesis allows us to use the basic method of analysis: construct a sequence of approximate solutions and show that this sequence converges to a solution.

It is crucial in this result that the norm comes from an inner product: the result is not true for arbitrary norms. For example, consider the closed unit ball in $\mathbb{R}^2$ for the supremum norm $\|(x,y)\|_\infty := \max\{|x|, |y|\}$ and $h = (2,0)$. In the proof of Theorem 1.1, the inner product does not appear explicitly, but enters via the parallelogram law.

*Proof of Theorem 1.1.* We construct a sequence $\{k_n\}$ of approximate solutions, prove that it is a Cauchy sequence, and argue that the limit $k$ is a solution. Because $d = d(h, S)$ is by definition a greatest lower bound, each $d + \frac{1}{n}$ is not a lower bound, and there is a sequence $\{k_n\} \subset S$ such that $d \le \|h - k_n\| \le d + \frac{1}{n}$. Notice that $\|h - k_n\| \to d$ by the squeeze principle. To get an expression for $\|k_m - k_n\|$, we apply the parallelogram law to $h - k_n$ and $h - k_m$:

$$\|(h - k_n) + (h - k_m)\|^2 + \|k_m - k_n\|^2 = 2(\|h - k_n\|^2 + \|h - k_m\|^2).$$

Since $(h - k_n) + (h - k_m) = 2(h - \frac{1}{2}(k_m + k_n))$ and $S$ is convex, we deduce that

$$\begin{aligned} \|k_m - k_n\|^2 &= 2(\|h - k_n\|^2 + \|h - k_m\|^2) - 4\|h - \tfrac{1}{2}(k_m + k_n)\|^2 \\ &\le 2(\|h - k_n\|^2 + \|h - k_m\|^2) - 4d^2, \end{aligned} \tag{1.1}$$

which converges to $2(d^2 + d^2) - 4d^2 = 0$ as $m, n \to \infty$. Thus $\{k_n\}$ is a Cauchy sequence[1].

Thus $\{k_n\}$ converges to a vector $k \in H$, which belongs to $S$ because $S$ is closed. Because subtraction and the norm are continuous (why?), $\|h-k_n\| \to \|h-k\|$, which together with $\|h-k_n\| \to d$ gives us $\|h-k\| = d$.

For the uniqueness, suppose there is another point $l$ such that $\|h-l\| = d$. Then $(k+l)/2$ also belongs to the convex set $S$, and $\|h - \frac{1}{2}(k+l)\| \geq d$ by definition of $d$. Another application of the parallelogram law gives

$$\begin{aligned} 2(d^2 + d^2) &= 2(\|h-k\|^2 + \|h-l\|^2) \\ &= \|(h-k) + (h-l)\|^2 + \|k-l\|^2 \\ &= \|2(h - \tfrac{1}{2}(k+l))\|^2 + \|k-l\|^2 \\ &\geq 4d^2 + \|k-l\|^2, \end{aligned}$$

which implies that $\|k-l\|^2 = 0$ and $k = l$. □

*Remark* 1.2. Notice that in the above proof we only used that if $h, k \in S$, then $\frac{1}{2}h + \frac{1}{2}k \in S$; that is, the definition of convexity with $t = \frac{1}{2}$. Indeed, it can be shown that $S$ is closed and convex if and only if $S$ is closed and $h, k \in S \implies \frac{1}{2}h + \frac{1}{2}k \in S$ for all $h, k \in S$.

Theorem 1.1 applies in particular to every closed subspace $M$ of a Hilbert space $H$. Drawing a few pictures in $\mathbb{R}^2$, where closed subspaces are lines through the origin, should convince you that the closest point in $M$ to $h$ can be obtained by dropping a perpendicular from $h$ to $M$. The next theorem says that these pictures give good intuition about what happens in general Hilbert spaces. To see why this might be powerful, note that part (a) relates the geometric notion of orthogonality to the metric notion of distance.

**Theorem 1.3.** *Suppose $M$ is a closed subspace of a Hilbert space $H$.*

(a) *If $h \in H$ and $k \in M$, then $\|h-k\| = d(h, M)$ if and only if $h - k \perp M$. (So that $k$ is the closest point of $M$ to $h$ if and only if $h-k$ is orthogonal to $M$.)*

(b) *For each $h \in H$, let $Ph$ denote the closest point in $M$ to $h$. Then $Ph$ is uniquely characterised by the properties that $Ph \in M$ and $h - Ph \perp M$. The function $P : H \to M$ has the following properties:*

(i) *$P : H \to M$ is linear;*
(ii) *$\|Ph\| \leq \|h\|$ for all $h$;*
(iii) *$P \circ P = P$;*

---

[1] In case this business about $m, n \to \infty$ makes you nervous, we include the details. Suppose $\epsilon > 0$ is given. Since $\|h-k_n\| \to d$, we have $\|h-k_n\|^2 \to d^2$ by the algebra of limits, and there exists $N \in \mathbb{N}$ such that

$$n \geq N \implies \|h-k_n\|^2 \leq d^2 + \epsilon^2/4.$$

Then from (1.1) we have

$$m, n \geq N \implies \|k_m - k_n\|^2 \leq 2(d^2 + \epsilon^2/4 + d^2 + \epsilon^2/4) - 4d^2 = \epsilon^2,$$

and $\{k_n\}$ is Cauchy.

(iv) $\ker P = M^\perp := \{h \in H : h \perp M\}$; *and*

(v) $\operatorname{range} P = M$.

*The map $P$ is called the* orthogonal projection *of $H$ onto $M$. $P$ is a bounded linear operator on $H$, $\|P\| = 0$ (iff $M = \{0\}$) or $\|P\| = 1$, and*

$$\|h\|^2 = \|Ph\|^2 + \|h - Ph\|^2 \quad \textit{for all } h \in H.$$

*Proof.* (a) Suppose first that $h - k \perp M$ and $z \in M$. Then $k - z \in M$, so Pythagoras's Theorem gives

$$\|h - z\|^2 = \|(h - k) + (k - z)\|^2 = \|h - k\|^2 + \|k - z\|^2 \geq \|h - k\|^2,$$

so $\|h - k\| = d(h, M)$, and $k$ is the closest point of $M$ to $h$.

Next suppose that $k$ is the closest point in $M$ to $h$, and $z \in M$. We want to show that $(h - k \mid z) = 0$. If $t \in \mathbb{R}$, then $k + tz \in M$ as $M$ is a subspace and

$$d^2 \leq \|h - (k + tz)\|^2 = \|(h - k) - tz\|^2 = d^2 + t^2\|z\|^2 - 2t(h - k \mid z).$$

Therefore,

$$t^2\|z\|^2 - 2t(h - k \mid z) \geq 0, \text{ for all } t \in \mathbb{R}. \tag{1.2}$$

If $t > 0$, then (1.2) implies that $t\|z\| \geq 2(h - k \mid z)$ for all $t > 0$ and hence, letting $t \to 0+$, it follows that $0 \geq (h - k \mid z)$. Similarly, if $t < 0$, then (1.2) implies that $t\|z\| \leq 2(h - k \mid z)$ for all $t < 0$ and hence, letting $t \to 0-$, it follows that $0 \leq (h - k \mid z)$. Thus $(h - k \mid z) = 0$.

(b) The characterisation of $Ph$ is a restatement of (a). For (i), suppose $h, k \in H$ and $c, d \in \mathbb{F}$. Then $c(Ph) + d(Pk) \in M$ and

$$\begin{aligned} h - Ph \text{ and } k - Pk \perp M &\Longrightarrow c(h - Ph) \text{ and } d(k - Pk) \perp M \\ &\Longrightarrow (ch + dk) - (c(Ph) + d(Pk)) \perp M. \end{aligned}$$

Thus $c(Ph) + d(Pk)$ has the properties which uniquely characterise $P(ch + dk)$, and we have $P(ch + dk) = c(Ph) + d(Pk)$, and $P$ is linear.

For (ii), we note that $h - Ph \in M^\perp$ and $Ph \in M$, so Pythagoras's Theorem implies

$$\|h\|^2 = \|(h - Ph) + Ph\|^2 = \|h - Ph\|^2 + \|Ph\|^2 \geq \|Ph\|^2. \tag{1.3}$$

For (iii) note that for all $h \in H$ we have that $Ph \in M$ and thus the closest point of $M$ to $Ph$ is $Ph$ itself. Therefore, $P(Ph) = Ph$ for all $h \in H$ and thus $P = P \circ P$.

For (iv) suppose $h \in H$. Then $Ph = 0$ iff $h - 0 \perp M$ iff $h \in M^\perp$.

For (v) we note that $\operatorname{range} P \subset M$ by definition. If $h \in M$ then the closest point of $M$ to $h$ is $h$ itself; that is, $h = Ph$. Thus $M \subset \operatorname{range} P$.

Equation (ii) imply that $P$ is bounded with $\|P\| \leq 1$; if $M = \{0\}$, then $Ph = 0$ for every $h$, and $\|P\| = \|0\|_{\text{op}} = 0$; if $M \neq \{0\}$, there is a unit vector $h \in M$, and then the equation $Ph = h$ implies $\|P\| = 1$. The last equality follows from Pythagoras's theorem. □

**Corollary 1.4.** *Suppose that $M$ is a closed subspace of a Hilbert space $H$ and let $h \in H$. Then $h$ can uniquely be written as $h = k + l$, where $k \in M$ and $l \in M^\perp$.*

*Proof.* If $h \in H$, then $h = Ph + h - Ph$. Thus we can take $k = Ph$ and $l = h - Ph$ where $Ph \in M$ and $h - Ph \in M^\perp$ by Theorem 1.3 (b). Suppose that $h = k_1 + l_1$ with $k_1 \in M$ and $l_1 \in M^\perp$. Then $0 = k - k_1 + l - l_1$ and thus

$$0 = \|k - k_1\|^2 + (k - k_1 \mid l - l_1) = \|k - k_1\|^2 + (k - k_1 \mid l) - (k - k_1 \mid l_1) = \|k - k_1\|^2.$$

Therefore, $k = k_1$ and $l = l_1$. □

We now discuss two important applications of Theorem 1.3. The first concerns the *orthogonal complement*

$$M^\perp := \{h \in H : (h \,|\, k) = 0 \text{ for all } k \in M\}$$

appearing in the Theorem. The linearity of the inner product implies that $M^\perp$ is a linear subspace of $H$, and the continuity of the inner product that it is closed: if $h_n \in M^\perp$ and $h_n \to h$ in $H$, then $(h_n \,|\, k) \to (h \,|\, k)$ implies $(h \,|\, k) = 0$ for all $k \in M$. So Theorem 1.3 says that there is an orthogonal projection onto $M^\perp$. To appreciate that the next Corollary might be saying something interesting, notice that the statement $(M^\perp)^\perp = M$ makes no explicit mention of closest points.

**Corollary 1.5.** *If $M$ is a closed subspace of $H$ and $P$ is the orthogonal projection of $H$ on $M$, then $I - P$ is the orthogonal projection of $H$ onto $M^\perp$, and $(M^\perp)^\perp = M$.*

*Proof.* For the first part, suppose $h \in H$. Then, for $z \in M^\perp$,

$$(h - (I - P)h \,|\, z) = (h - h + Ph \,|\, z) = (Ph \,|\, z) = 0,$$

so $I - P$ has the property characterising the projection on $M^\perp$. Part (iv) of the Theorem now implies $(M^\perp)^\perp = \ker(I - P)$. But

$$k \in \ker(I - P) \Longleftrightarrow (I - P)k = 0 \Longleftrightarrow Pk = k \Longleftrightarrow k \in M,$$

so $\ker(I - P) = M$, and we are done. □

*Remark.* We stress that the (orthogonal) complement $M^\perp$ is *not* the same as the set-theoretic complement $H \setminus M = \{h \in H : h \notin M\}$. For example, the orthogonal complement of the $x$-axis in the inner-product space $\mathbb{R}^2$ is the $y$-axis.