Proving Things

Stéphane Dupraz

1 Using and Proving Implications and Equivalences

Let P and Q be two statements.

- We say that "P implies Q", or "if P then Q", and note $P \Rightarrow Q$, if Q is true when P is true.
- We say that P is a **sufficient condition** for Q, and Q is a **necessary condition** for P.
- P does not imply Q if P is true but Q is false.
- $P \Rightarrow Q$ and $Q \Rightarrow P$ are two very different statements. We call one the **converse** of the other.
- We say that "P and Q are **equivalent**", or "P if and only if (iff) Q", and note $P \Leftrightarrow Q$, if P implies Q and Q implies P.
- The implication $P \Rightarrow Q$ is equivalent to its **contrapositive** not(Q) $\Rightarrow$ not(P).

The basis of deductive reasoning is quite simple. If we know a statement P to be true, and a statement (P $\Rightarrow$ Q) to be true, then Q is true. This is how we use implications. Proving an implication is about as simple: we assume that P is true, and show that Q is true. Given the definition of an inclusion, proving an inclusion is one particular case of proving an implication.

Example 1. *Let us prove for instance that for a function $f : X \to Y$ and two subsets of Y, T_1 and T_2, $f^{-1}(T_1 \cap T_2) \subseteq f^{-1}(T_1) \cap f^{-1}(T_2)$. This means showing for $x \in X$:*

$$x \in f^{-1}(T_1 \cap T_2) \Rightarrow x \in f^{-1}(T_1) \cap f^{-1}(T_2)$$

Assume $x \in f^{-1}(T_1 \cap T_2)$. By definition of the inverse image, this means $f(x) \in T_1 \cap T_2$. Since $f(x) \in T_1$, $x \in f^{-1}(T_1)$. Since $f(x) \in T_2$, $x \in f^{-1}(T_2)$. So $x \in f^{-1}(T_1) \cap f^{-1}(T_2)$. QED.

Sometimes, it is easier (or even only possible) to prove the implication $P \Rightarrow Q$ by proving its contrapositive not(Q) $\Rightarrow$ not(P). We call it a **proof by contrapositive**.

An equivalence consists of two implications. To use an equivalence in a proof, we just need to decide which implication is going to be useful. To show an equivalence, we show both implications (to prove an equality of sets, we show both inclusions).

Example 2. *Let us prove that $f^{-1}(T_1 \cap T_2) = f^{-1}(T_1) \cap f^{-1}(T_2)$. We have proven the first inclusion in the previous example. We show the converse:*

$$x \in f^{-1}(T_1) \cap f^{-1}(T_2) \Rightarrow x \in f^{-1}(T_1 \cap T_2)$$

Assume $x \in f^{-1}(T_1) \cap f^{-1}(T_2)$. Since $x \in f^{-1}(T_1)$, $f(x) \in T_1$. Since $x \in f^{-1}(T_2)$, $f(x) \in T_2$. So $f(x) \in T_1 \cap T_2$. Hence, $x \in f^{-1}(T_1 \cap T_2)$.

Alternatively however, it is sometimes possible to show an equivalence through a series of equivalences. If P $\Leftrightarrow R_1$, $R_1 \Leftrightarrow R_2$, ..., $R_{n-1} \Leftrightarrow R_n$, and $R_n \Leftrightarrow Q$, then $P \Leftrightarrow Q$. This requires to be very careful that each equivalence goes indeed "both ways" and is not only an implication.

Example 3. *Let us prove for instance that $f^{-1}(T_1 \cap T_2) = f^{-1}(T_1) \cap f^{-1}(T_2)$ through a series of equivalences:*

$$\begin{aligned} x \in f^{-1}(T_1 \cap T_2) &\Leftrightarrow f(x) \in T_1 \cap T_2 \\ &\Leftrightarrow f(x) \in T_1 \text{ and } f(x) \in T_2 \\ &\Leftrightarrow x \in f^{-1}(T_1) \text{ and } x \in f^{-1}(T_2) \\ &\Leftrightarrow x \in f^{-1}(T_1) \cap f^{-1}(T_2) \end{aligned}$$

2 Quantifiers

Many of the difficulties in doing proofs have to do with dealing with the statements "for all" and "there exists": the universal and existential quantifiers. Let $P(x), x \in X$ be a family of statements. We consider two new statements:

- The statement "for all $x \in X, P(x)$" is true if $P(x)$ is true for all $x \in X$, and is false if there exists an x such that $P(x)$ is false. We note "$\forall x, P(x)$" and call "for all" ($\forall$) the **universal quantifier**.
- The statement "there exists an $x \in X$ such that $P(x)$" is true if there exists an $x \in X$ such that $P(x)$, and is false if $P(x)$ is false for all $x \in X$. We note "$\exists x / P(x)$" and call "there exists" ($\exists$) the **existential**

quantifier.

- "$\exists x \in X/P(x)$" does not mean that the x such that $P(x)$ is true is unique. To denote that there exists a unique $x \in X$ such that $P(x)$, we note $\exists! x/P(x)$.

If P is a statement, the **negation** of P, not(P), is true when P is false and false when P is true. Notice that the negation "reverses the quantifiers":

$$\text{not}(\exists x \in X/\ \text{P(x)}) \text{ is equivalent to } \forall x \in X,\ \text{not}(P(x))$$
$$\text{not}(\forall x \in X,\ \text{P(x)}) \text{ is equivalent to } \exists x \in X/\ \text{not}(P(x))$$

In words, to prove that "$\forall x, P(x)$" is false, we exhibit a **counter-example**. Exercises are sometimes phrased "Provide a proof if it is true, and a counter-example if it is false"; but "prove your answer" is an equivalent requirement, as providing a counter-example proves the negation.

It is sometimes useful to apply these rules mechanically to rewrite the formulation of a statement that involves several quantifiers. For instance, take the definition of the convergence of a sequence in $\mathbb{R}$. A sequence $(x_n) \in \mathbb{R}^{\mathbb{N}}$ converges to a limit $l \in \mathbb{R}$ iff:

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}/\forall n \geq N, |x_n - l| < \varepsilon$$

The sequence (x_n) does not converge to the limit l iff:

$$\exists \varepsilon > 0/\forall N \in \mathbb{N}, \exists n \geq N/|x_n - l| \geq \varepsilon$$

3 Dealing with Quantifiers in Proofs

Proving or using statements with the universal or existential quantifiers involve completely different methods.

3.1 Proving a $\forall$

To prove a statement of the form "$\forall x \in X, P(x)$", we just fix an $x \in X$, and prove $P(x)$, being careful to use a reasoning that applies to any $x \in X$. This is usually straightforward; we have done it in the examples above.

3.2 Proving a $\exists$

Proving a statement of the form "$\exists x \in X/P(x)$" is more difficult. We need to point at an x that works—that satisfies P(x); this is easier said than done.

Example 4. *Let us prove that if f is bijective, then f has an inverse. Assume f is bijective; we want to show that there exists a function $g : Y \to X$ such that $f \circ g = Id_X$ and $g \circ f = Id_Y$.*

Let $y \in Y$. Since f is surjective and y is in the image of X, there exists $x \in X$ such that $y = f(x)$. Let us define this x as $g(y)$. We have that $y = f(g(y))$. Since f is injective, the x such that $y = f(x)$ is unique. So $g(f(x)) = x$. Since y was any element of Y, $Id_Y = f \circ g$ and $g \circ f = Id_X$. QED.

3.3 Using a $\exists$

To use an assumption of the form "$\exists x \in X, P(x)$" in a proof, we just welcome the manna from heaven x that satisfies $P(x)$ and seek to do something relevant with it in order to complete the proof. We did it in the previous example when using the existence of an x such that $y = f(x)$.

3.4 Using a $\forall$

Using an assumption of the form "$\forall x \in X, P(x)$" in a proof is more difficult, because we need to choose which x to apply $P(x)$ to.

Example 5. *Let use prove that $S_1 \subseteq S_2 \Rightarrow f(S_1) \subseteq f(S_2)$. Note that $S_1 \subseteq S_2$ contains a $\forall$ quantifier since it means:*

$$\forall x \in X, x \in S_1 \Rightarrow x \in S_2$$

Assume $S_1 \subseteq S_2$. Let $y \in f(S_1)$. We want to show that $y \in f(S_2)$. Since $y \in f(S_1)$, by definition there exists $x \in S_1$ such that $y = f(x)$. Since $S_1 \subseteq S_2$, $x \in S_2$, so that $y = f(x) \in f(S_2)$. QED.

Here, we applied the assumption to the x such that $y = f(x)$.

3.5 Proving uniqueness

To show that "$\exists! x / P(x)$", show existence and uniqueness separately. To show uniqueness, assume there exist two x such that $P(x)$ and show that they are equal.

Example 6. *Let us prove the uniqueness of the inverse of a function. Assume g and g' are two inverses of a function $f : X \to Y$. Since g is an inverse of f, $f \circ g = Id_Y$. Compose by g' to the left: $g' \circ f \circ g = g'$. Since g' is an inverse of f, $g' \circ f = Id_X$. Applied to the previous equality, $Id_X \circ g = g'$, i.e $g = g'$. QED.*

4 Proof by contradiction

A **proof by contradiction** is sometimes very helpful, as standard methods of proofs do not work. To prove P by contradiction, we assume not(P) and derive true statements until we end up proving that a statement we know to be true is false (this can be any statement in the mathematical edifice).

Example 7. *A function f is strictly concave if for all $x, y \in X$ such that $x \neq y$, and all $\lambda \in (0,1)$, $f(\lambda x + (1-\lambda)y) > \lambda f(x) + (1-\lambda)f(y)$. We show by contradiction that f cannot have two (distinct) maximizers.*

Assume f has two maximizers x and y, $x \neq y$. Then for $\lambda = 1/2$, $f(\frac{x+y}{2}) > \frac{1}{2}f(x) + \frac{1}{2}f(y) = f(x)$, which contradicts that x is a maximizer of f. QED.

However powerful proofs by contradiction may be, be careful not to overuse them. It is always possible to turn a standard proof into a proof by contradiction. It results in a logically valid proof, but usually also a much less intuitive proof. Try to reserve proofs by contradiction to when there exists no alternative.

5 Proof by induction

Finally, a specific type of proof is possible for statements of the form:

$$\forall n \in \mathbb{N}, P(n)$$

(A proof by induction also works for statements of the form "$\forall n \geq N, P(n)$" for some integer N).

To prove this by induction, we prove two things:

1. The **base case**: we prove P(0) (or P(N) more generally).
2. The **inductive step**: we prove that $P(n)$ implies P(n+1) for all $n \in \mathbb{N}$ (or for all $n \geq N$ more generally).

Example 8. *Let A, B, P be $n \times n$ matrices, with P invertible. We show that if $A = P^{-1}BP$ then for all $k \geq 1$, $A^k = P^{-1}B^kP$.*

1. *The base case is the assumption of the implication.*
2. *Fix $k \geq 1$ and assume that $A^k = P^{-1}B^kP$. We have:*

$$A^{k+1} = A^k \times A = (P^{-1}B^kP)(P^{-1}BP) = P^{-1}B^kBP = P^{-1}B^{k+1}P.$$