prf.1 Inference Patterns

mth:prf:pat:sec

Proofs are composed of individual inferences. When we make an inference, we typically indicate that by using a word like "so," "thus," or "therefore." The inference often relies on one or two facts we already have available in our proof—it may be something we have assumed, or something that we've concluded by an inference already. To be clear, we may label these things, and in the inference we indicate what other statements we're using in the inference. An inference will often also contain an explanation of *why* our new conclusion follows from the things that come before it. There are some common patterns of inference that are used very often in proofs; we'll go through some below. Some patterns of inference, like proofs by induction, are more involved (and will be discussed later).

We've already discussed one pattern of inference: unpacking, or applying, a definition. When we unpack a definition, we just restate something that involves the definiendum by using the definiens. For instance, suppose that we have already established in the course of a proof that $U = V$ (a). Then we may apply the definition of $=$ for sets and infer: "Thus, by definition from (a), every element of U is an element of V and vice versa."

Somewhat confusingly, we often do not write the justification of an inference when we actually make it, but before. Suppose we haven't already proved that $U = V$, but we want to. If $U = V$ is the conclusion we aim for, then we can restate this aim also by applying the definition: to prove $U = V$ we have to prove that every element of U is an element of V and vice versa. So our proof will have the form: (a) prove that every element of U is an element of V; (b) every element of V is an element of U; (c) therefore, from (a) and (b) by definition of $=$, $U = V$. But we would usually not write it this way. Instead we might write something like,

> We want to show $U = V$. By definition of $=$, this amounts to showing that every element of U is an element of V and vice versa.
>
> (a) ... (a proof that every element of U is an element of V) ...
>
> (b) ... (a proof that every element of V is an element of U) ...

Using a Conjunction

Perhaps the simplest inference pattern is that of drawing as conclusion one of the conjuncts of a conjunction. In other words: if we have assumed or already proved that p and q, then we're entitled to infer that p (and also that q). This is such a basic inference that it is often not mentioned. For instance, once we've unpacked the definition of $U = V$ we've established that every element of U is an element of V and vice versa. From this we can conclude that every element of V is an element of U (that's the "vice versa" part).

Proving a Conjunction

Sometimes what you'll be asked to prove will have the form of a conjunction; you will be asked to "prove p and q." In this case, you simply have to do two things: prove p, and then prove q. You could divide your proof into two sections, and for clarity, label them. When you're making your first notes, you might write "(1) Prove p" at the top of the page, and "(2) Prove q" in the middle of the page. (Of course, you might not be explicitly asked to prove a conjunction but find that your proof requires that you prove a conjunction. For instance, if you're asked to prove that $U = V$ you will find that, after unpacking the definition of $=$, you have to prove: every element of U is an element of V *and* every element of V is an element of U).

Proving a Disjunction

When what you are proving takes the form of a disjunction (i.e., it is an statement of the form "p or q"), it is enough to show that one of the disjuncts is true. However, it basically never happens that either disjunct just follows from the assumptions of your theorem. More often, the assumptions of your theorem are themselves disjunctive, or you're showing that all things of a certain kind have one of two properties, but some of the things have the one and others have the other property. This is where proof by cases is useful (see below).

Conditional Proof

Many theorems you will encounter are in conditional form (i.e., show that if p holds, then q is also true). These cases are nice and easy to set up—simply assume the antecedent of the conditional (in this case, p) and prove the conclusion q from it. So if your theorem reads, "If p then q," you start your proof with "assume p" and at the end you should have proved q.

Recall that a biconditional (p iff q) is really two conditionals put together: if p then q, and if q then p. All you have to do, then, is two instances of conditional proof: one for the first instance and one for the second. Sometimes, however, it is possible to prove an "iff" statement by chaining together a bunch of other "iff" statements so that you start with "p" an end with "q"—but in that case you have to make sure that each step really is an "iff."

Universal Claims

Using a universal claim is simple: if something is true for anything, it's true for each particular thing. So if, say, the hypothesis of your proof is $X \subseteq Y$, that means (unpacking the definition of $\subseteq$), that, for every $x \in X$, $x \in Y$. Thus, if you already know that $z \in X$, you can conclude $z \in Y$.

Proving a universal claim may seem a little bit tricky. Usually these statements take the following form: "If x has P, then it has Q" or "All Ps are Qs." Of course, it might not fit this form perfectly, and it takes a bit of practice

to figure out what you're asked to prove exactly. But: we often have to prove that all objects with some property have a certain other property.

The way to prove a universal claim is to introduce names or variables, for the things that have the one property and then show that they also have the other property. We might put this by saying that to prove something for *all* Ps you have to prove it for an *arbitrary* P. And the name introduced is a name for an arbitrary P. We typically use single letters as these names for arbitrary things, and the letters usually follow conventions: e.g., we use n for natural numbers, φ for formulas, X for sets, f for functions, etc.

The trick is to maintain generality throughout the proof. You start by assuming that an arbitrary object ("x") has the property P, and show (based only on definitions or what you are allowed to assume) that x has the property Q. Because you have not stipulated what x is specifically, other that it has the property P, then you can assert that all every P has the property Q. In short, x is a stand-in for *all* things with property P.

Proposition prf.1. *For all sets X and Y, $X \subseteq X \cup Y$.*

Proof. Let X and Y be arbitrary sets. We want to show that $X \subseteq X \cup Y$. By definition of $\subseteq$, this amounts to: for every x, if $x \in X$ then $x \in X \cup Y$. So let $x \in X$ be an arbitrary element of X. We have to show that $x \in X \cup Y$. Since $x \in X$, $x \in X$ or $x \in Y$. Thus, $x \in \{x : x \in X \vee x \in Y\}$. But that, by definition of $\cup$, means $x \in X \cup Y$. □

Proof by Cases

Suppose you have a disjunction as an assumption or as an already established conclusion—you have assumed or proved that p or q is true. You want to prove r. You do this in two steps: first you assume that p is true, and prove r, then you assume that q is true and prove r again. This works because we assume or know that one of the two alternatives holds. The two steps establish that either one is sufficient for the truth of r. (If both are true, we have not one but two reasons for why r is true. It is not necessary to separately prove that r is true assuming both p and q.) To indicate what we're doing, we announce that we "distinguish cases." For instance, suppose we know that $x \in Y \cup Z$. $Y \cup Z$ is defined as $\{x : x \in Y \text{ or } x \in Z\}$. In other words, by definition, $x \in Y$ or $x \in Z$. We would prove that $x \in X$ from this by first assuming that $x \in Y$, and proving $x \in X$ from this assumption, and then assume $x \in Z$, and again prove $x \in X$ from this. You would write "We distinguish cases" under the assumption, then "Case (1): $x \in Y$" underneath, and "Case (2): $x \in Z$ halfway down the page. Then you'd proceed to fill in the top half and the bottom half of the page.

Proof by cases is especially useful if what you're proving is itself disjunctive. Here's a simple example:

Proposition prf.2. *Suppose $Y \subseteq U$ and $Z \subseteq V$. Then $Y \cup Z \subseteq U \cup V$.*

Proof. Assume (a) that $Y \subseteq U$ and (b) $Z \subseteq V$. By definition, any $x \in Y$ is also $\in U$ (c) and any $x \in Z$ is also $\in V$ (d). To show that $Y \cup Z \subseteq U \cup V$, we have to show that if $x \in Y \cup Z$ then $x \in U \cup V$ (by definition of $\subseteq$). $x \in Y \cup Z$ iff $x \in Y$ or $x \in Z$ (by definition of $\cup$). Similarly, $x \in U \cup V$ iff $x \in U$ or $x \in V$. So, we have to show: for any x, if $x \in Y$ or $x \in Z$, then $x \in U$ or $x \in V$.

> So far we've only unpacked definitions! We've reformulated our proposition without $\subseteq$ and $\cup$ and are left with trying to prove a universal conditional claim. By what we've discussed above, this is done by assuming that x is something about which we assume the "if" part is true, and we'll go on to show that the "then" part is true as well. In other words, we'll assume that $x \in Y$ or $x \in Z$ and show that $x \in U$ or $x \in V$.[1]

Suppose that $x \in Y$ or $x \in Z$. We have to show that $x \in U$ or $x \in V$. We distinguish cases.

Case 1: $x \in Y$. By (c), $x \in U$. Thus, $x \in U$ or $x \in V$. (Here we've made the inference discussed in the preceding subsection!)

Case 2: $x \in Z$. By (d), $x \in V$. Thus, $x \in U$ or $x \in V$. □

Proving an Existence Claim

When asked to prove an existence claim, the question will usually be of the form "prove that there is an x such that $\ldots x \ldots$", i.e., that some object that has the property described by "$\ldots x \ldots$". In this case you'll have to identify a suitable object show that is has the required property. This sounds straightforward, but a proof of this kind can be tricky. Typically it involves *constructing* or *defining* an object and proving that the object so defined has the required property. Finding the right object may be hard, proving that it has the required property may be hard, and sometimes it's even tricky to show that you've succeeded in defining an object at all!

Generally, you'd write this out by specifying the object, e.g., "let x be $\ldots$" (where $\ldots$ specifies which object you have in mind), possibly proving that $\ldots$ in fact describes an object that exists, and then go on to show that x has the property Q. Here's a simple example.

Proposition prf.3. *Suppose that $x \in Y$. Then there is an X such that $X \subseteq Y$ and $X \neq \emptyset$.*

Proof. Assume $x \in Y$. Let $X = \{x\}$.

> Here we've defined the set X by enumerating its elements. Since we assume that x is an object, and we can always form a set by enumerating its elements, we don't have to show that we've succeeded in defining a set X here. However, we still have to show

[1] This paragraph just explains what we're doing—it's not part of the proof, and you don't have to go into all this detail when you write down your own proofs.

that X has the properties required by the proposition. The proof isn't complete without that!

Since $x \in X$, $X \neq \emptyset$.

> This relies on the definition of X as $\{x\}$ and the obvious facts that $x \in \{x\}$ and $x \notin \emptyset$.

Since x is the only element of $\{x\}$, and $x \in Y$, every element of X is also an element of Y. By definition of $\subseteq$, $X \subseteq Y$. □

Using Existence Claims

Suppose you know that some existence claim is true (you've proved it, or it's a hypothesis you can use), say, "for some x, $x \in X$" or "there is an $x \in X$." If you want to use it in your proof, you can just pretend that you have a name for one of the things which your hypothesis says exist. Since X contains at least one thing, there are things to which that name might refer. You might of course not be able to pick one out or describe it further (other than that it is $\in X$). But for the purpose of the proof, you can pretend that you have picked it out and give a name to it. It's important to pick a name that you haven't already used (or that appears in your hypotheses), otherwise things can go wrong. In your proof, you indicate this by going from "for some x, $x \in X$" to "Let $a \in X$." Now you can reason about a, use some other hypotheses, etc., until you come to a conclusion, p. If p no longer mentions a, p is independent of the asusmption that $a \in X$, and you've shown that it follows just from the assumption "for some x, $x \in X$."

Proposition prf.4. *If $X \neq \emptyset$, then $X \cup Y \neq \emptyset$.*

Proof. Suppose $X \neq \emptyset$. So for some x, $x \in X$.

> Here we first just restated the hypothesis of the proposition. This hypothesis, i.e., $X \neq \emptyset$, hides an existential claim, which you get to only by unpacking a few definitions. The definition of $=$ tells us that $X = \emptyset$ iff every $x \in X$ is also $\in \emptyset$ and every $x \in \emptyset$ is also $\in X$. Negating both sides, we get: $X \neq \emptyset$ iff either some $x \in X$ is $\notin \emptyset$ or some $x \in \emptyset$ is $\notin X$. Since nothing is $\in \emptyset$, the second disjunct can never be true, and "$x \in X$ and $x \notin \emptyset$" reduces to just $x \in X$. So $x \neq \emptyset$ iff for some x, $x \in X$. That's an existence claim. Now we use that existence claim by introducing a name for one of the elements of X:

Let $a \in X$.

> Now we've introduced a name for one of the things $\in X$. We'll continue to argue about a, but we'll be careful to only assume that $a \in X$ and nothing else:

Since $a \in X$, $a \in X \cup Y$, by definition of $\cup$. So for some x, $x \in X \cup Y$, i.e., $X \cup Y \neq \emptyset$.

> In that last step, we went from "$a \in X \cup Y$" to "for some x, $x \in X \cup Y$." That doesn't mention a anymore, so we know that "for some x, $x \in X \cup Y$" follows from "for some x, $x \in X$ alone." But that means that $X \cup Y \neq \emptyset$.

□

It's maybe good practice to keep bound variables like "x" separate from hypothtical names like a, like we did. In practice, however, we often don't and just use x, like so:

> Suppose $X \neq \emptyset$, i.e., there is an $x \in X$. By definition of $\cup$, $x \in X \cup Y$. So $X \cup Y \neq \emptyset$.

However, when you do this, you have to be extra careful that you use different x's and y's for different existential claims. For instance, the following is *not* a correct proof of "If $X \neq \emptyset$ and $Y \neq \emptyset$ then $X \cap Y \neq \emptyset$" (which is not true).

> Suppose $X \neq \emptyset$ and $Y \neq \emptyset$. So for some x, $x \in X$ and also for some x, $x \in Y$. Since $x \in X$ and $x \in Y$, $x \in X \cap Y$, by definition of $\cap$. So $X \cap Y \neq \emptyset$.

Can you spot where the incorrect step occurs and explain why the result does not hold?

Photo Credits

Bibliography