Intro to Mathematical Reasoning (Math 300)

Supplement 5. Proofs: structure and strategy [1]

In this supplement, we will look more systematically at the structure of proofs, and permissible strategies.

1 Objects and assumptions

Two crucial ingredients of a mathematical proof are: (1) the objects referred to in the proof (2) the assumptions made during the proof.

As discussed in supplement 4, the mathematical objects in a proof play a role that is analogous to the role of the characters in a novel. Recall that the first rule of working with objects in a mathematical proof is that each object that you wish to talk about in the proof must be given a name that is introduced with a "Let ..." statement. Each object name has a life span during which it is active. In any sentence that appears in your proof, the letters that occur in that sentence are either dummy variables or active object names.

The assumptions in a proof are pieces of information that may be treated as true within the proof (or within a portion of the proof.) For example, whenever you introduce an object name, the introduction provides you with information about the object being introduced which can be used later in the proof. If you introduce the object name x by saying: "Let x be a real number greater than 1", the information "x is a real number greater than 1" is an assumption.

There are other situations (discussed in the rest of this supplement) where you are permitted to make assumptions in a proof. For example, when you prove a statement of the form "if A then B", you are allowed to assume A. Every assumption, like every object, has a life span, which is determined by the rules of proof. During the life span of the assumption, you may use the assumption as if it were true.

2 The four types of sentences in a proof

A proof consists of a sequence of sentences. Each sentence has a purpose within the proof. There are four basic sentence types in a proof (though a sentence may sometimes combine two or more types):

- *Object name introduction.* This is a usually sentence of the form "Let x be ...."
- *Assumption.* A sentence of the form "Assume A" where A is either a statement, or a predicate involving object names that are currently active. For example, if r, s were introduced as real numbers, you might have a sentence "Assume $r > s$." in your proof. (The rules for this will be explained below.)
- *Deduction.* A new statement, or predicate involving currently active object names is deduced using known facts, assumptions, definitions and logic. Such a sentence should include an explanation of what facts and principles are used (unless it is obvious). For example, suppose that a, b, c are active object names each representing real numbers, and $a = 2b + 4$ and

[1] Version 2/4/04.

$b = 3c - 7$ are among the list of assumptions. Then we might write "Since $a = 2b + 4$ and $b = 3c - 7$ we can substitute $3c - 7$ for b in the first equation to obtain $a = 6c - 10$."

- *Trail markers: explanations and reminders.* In writing an informal proof, you should include extra sentences that serve as "trail markers" that make it easier for the reader to follow the proof. For example, you might include sentences that explain why you are taking the steps you are taking and sentences that remind the reader about a definition or a previously proved theorem that you want to apply in your proof.

Let's look at a simple proof and classify the sentences in it. First a definition: we say that an integer s is a square provided that there is an integer p such that $p^2 = s$. "For all squares r and s, $r \times s$ is a square".

> Let a and b be squares. We will now show that $a \times b$ is a square. To do this, we will prove that there is an integer p such that $p^2 = ab$. By the definition of square, this will prove that ab is a square.
>
> Since a is a square, by definition, there is an integer, we will call t, such that $t^2 = a$. Since b is a square there is an integer u such that $u^2 = b$. Since t and u are integers, tu is an integer and also $(tu)^2 = t^2u^2 = ab$. So we have shown that there is an integer p such that $p^2 = ab$.
>
> Therefore, for all squares r and s, rs is a square.

Let's classify the sentences of this proof. In the first paragraph the first sentence is an object name introduction. The next two sentences are explanations.

In the second paragraph, the first sentence is both a deduction (about a, using the definition of "square") and an introduction (of t). Similarly, the second sentence is both a deduction and an introduction.

The rest of the sentences in the proof are deductions.

3 Transforming your goal

When you write a proof, your goal is to demonstrate that a particular mathematical statement is true. One of the major techniques for proof is *transforming your goal*, that is, changing what you want to prove to something else. In the previous example, we started with the goal of proving the statement "For all squares r and s, $r \times s$ is a square". We introduce a and b to be squares and we transform the goal to proving "There is an integer p such that $p^2 = ab$".

Notice that, in this case, the new sentence to be proved is not a mathematical statement; it is a predicate with free variables a and b and dummy variable (or bound variable) p. Proving the predicate "There is an integer p such that $p^2 = ab$" means demonstrating that the predicate is true whenever a and b are replaced by specific values they satisfy the currently active assumptions for a and b. In this case the active assumptions are that a and b are both squares.

In this way, it makes sense to talk about proving a predicate, provided that all of the free variables in the predicate are currently active object names. A predicate all of whose free variables are active object names is called an *instantiated predicate*.

4 Choosing proof strategy based on the top-level structure

Recall that in Supplement 2 we learned about the seven basic ways of building up complex statements from simpler ones: negation, one of the four logical connectives "and", "or", "if – then", and "if and only if", universal quantification, and existential quantification. We said that a predicate is called *primitive* if it does not use any of these. We learned how to parse statements and predicates into their primitive components. We defined the "top-level structure" of a statement or predicate to be the compressed representation of the predicate at the top (or final) node of the parse tree.

For example, the predicate,

$x \in S$ and for all y belonging to S, $y \geq x$

has top-level structure

$A(x, S)$ and $B(x, S)$

where $A(x, S)$ is the predicate "$x \in S$" and $B(x, S)$ is the predicate "for all y belonging to S, $y \geq x$".

We also learned about pushing negations through a sentence.

Predicates that are not primitive are classified into types according to the operation that occurs in the top-level structure. Thus the example above would be classified as an "and" type of predicate. The proper proof strategy to be used in a proof is often determined by the top-level operation.

Before trying to prove a statement, you should push negations through. Once this is done then you get either (1) a primitive statement, (2) the negation of a primitive statement or (3) a statement whose top-level operation is either a quantifier or a logical connective.

Here are the main permissible proof strategies associated with the different top-level structures. (There are others, but we concentrate on these for now.)

Existential quantification To prove something of the form "There exists an x satisfying $A(x)$", the standard method is:

1. Introduce an object t, giving precise instructions for selecting t, and proving that it is possible to carry out the instructions.
2. Prove $A(t)$.
3. Conclusion: There exists x satisfying $A(x)$.

(At the end of this proof, t is no longer an active object.)

Universal quantification.

To prove something of the form "For all x, satisfying $H(x)$, $C(x)$ holds.", the standard method is the *arbitrary value method*

1. Let a be an arbitrary object satisfying $H(a)$.
2. Prove $C(a)$.
3. Conclusion: For all x satisfying $H(x)$, $C(x)$ holds.

(At the end of this proof, a is no longer an active object.)

Statements whose top-level structure is universal and whose next level structure is existential are "universal–existential" statements. The proof strategy for such statements is obtained by combining the above two proof strategies:

Universal–Existential quantification. To prove a statement of the form "For all x satisfying $H(x)$ there exists y such that x and y together satisfy $C(x, y)$."

1. Let a be an arbitrary object satisfying $H(a)$.
2. Introduce an object b, giving precise instructions for selecting b, and proving that it is possible to carry out the instructions. Usually the instructions for b depend on the value of a.
3. Prove $C(a, b)$.
4. Conclusion: "For all x satisfying $H(x)$ there exists y such that x and y together satisfy $C(x, y)$."

(At the end of this proof, a and b are no longer active objects.)

Logical connective "and". To prove something of the form "A and B", the standard method is:

1. Prove A.
2. Separately, prove B.
3. Conclusion: A and B.

(Any objects introduced or assumptions made while proving A are active only during the proof of A, and can not be used in the proof of B.)

Logical connective "If–then" Suppose the top-level structure of what you are trying to prove is "if A then B". Here are two valid proof strategies for this:

1. Assume A.
2. Prove B.
3. Conclusion: If A then B.

(After completion of the proof, the assumption A is no longer active.)

The second proof strategy for "if–then" is:

1. Assume $\sim B$.
2. Prove $\sim A$.
3. Conclusion: If A then B.

After completion of the proof, the assumption $\sim B$ is no longer active.

(**Warning**: The following is *not* a valid proof strategy for "if A then B" (1) Assume B, (2) Prove A.)

Logical connective "If and only if". Suppose you are trying to prove something of the form: "A if and only if B". This is equivalent to "(if A then B) and (if B then A)", so we can use the proof strategy associated with "and".

1. Prove "if A then B".
2. Prove "if B then A".
3. Conclusion: A if and only if B.

(Any objects introduced or assumptions made during the proof of "if A then B" are active only during the proof of that part, and can not be used in the proof of "if B then A".)

Logical connective "or". Suppose you are trying to prove something of the form: "A or B". This is logically equivalent to "if $\sim A$ then B" and so we can use one of the two proof strategies for "if – then":

1. Assume $\sim A$.
2. Prove B.
3. Conclusion:A or B.

(After completion of the proof, the assumption $\sim A$ is no longer active.)

Another form:

1. Assume $\sim B$.
2. Prove A.
3. Conclusion:A or B.

(After completion of the proof, the assumption $\sim B$ is no longer active.)

Here are a few comments about the strategies described above.

1. The proof strategies for "and" and for "if and only if" involve splitting what you are proving into two separate parts and proving each one.
2. The proof strategy used to prove a statement is almost always different from the proof strategy used to disprove the statement. When you disprove A, you must prove $\sim A$. To prove $\sim A$ you must first push negations to obtain an equivalent statement B, and the structure of B is what determines your proof. For example, when you prove a universal statement you use the arbitrary value method. When you disprove a universal statement, you are proving an existential statement, so you use the proof strategy for existential statements.

5 Making an assumption

The proof strategies presented above for "if–then" and "or" allow you to make an assumption. As we discussed earlier, when you make an assumption according to the rules of proof, then as long as that assumption is active, you may treat that assumption as though it were true.

There are two other forms that may be used in a proof that involve assumptions. These proof strategies may be used regardless of the top-level structure of the statement you are trying to prove.

The first is:

"Proof by cases" strategy, basic version. If you are trying to prove A, and B is any predicate involving only active object names, then the following is a valid strategy:

1. Split proof into two cases: B and $\sim B$.
2. Case 1.
   (a) Assume B.
   (b) Prove A.
3. Case 2.
   (a) Assume $\sim B$.
   (b) Prove A.
4. Conclusion: A.

(Any objects introduced or assumptions made during the proof of Case 1 are active only during the proof of that case, and can not be used in the proof of Case 2.)

"Proof by cases" strategy, general version If you are trying to prove A, and $B_1, B_2, ..., B_k$ is a list of k predicates where k is an integer involving only active object names, then the following is a valid strategy:

1. Prove $B_1 \vee B_2 \vee \cdots \vee B_k$ (at least one of B_1,B_2,..., B_k must be true).
2. Split proof into k cases. In case j (where j is an integer between 1 and k):
   (a) Assume B_j.
   (b) Prove A.
3. Conclusion: A.

(Any objects introduced or assumptions made during the proof of any case is active only during the proof of that case and may not be used in the proof of another case.)

When using proof by cases, the choice of B (in the basic version) and of $B_1, \ldots, B_k$ in the general version, is completely up to you. However, you only want to use proof by cases if splitting into cases helps, by making the proof easier.

Here is another proof strategy that involves making an assumption.

Proof by contradiction Suppose you are trying to prove A. A valid proof strategy for this is:

1. Assume A is not true.
2. Show that this assumption leads to a contradiction.
3. Conclusion: A is true.

Here by a contradiction we mean that for some statement (or instantiated predicate) B you prove that, assuming $\sim A$, both B and $\sim B$ are true. This is clearly impossible and therefore $\sim A$ must be false and so A must be true.

6 An example

In this section, we prove a simple theorem to illustrate the use of a number of these proof strategies.

> **Definition.** For real numbers x, y the *closed interval from x to y*, denoted $[x, y]$, is defined to be the set of real numbers z that satisfy $z \geq x$ and $z \leq y$.

Observe that the interval $[x, y]$ is a nonempty set if $x \leq y$ and is the empty set if $y < x$.

Now suppose that we have four numbers x, y, z, w satisfying $x \leq y$ and $z \leq w$ so that the two closed intervals $[x, y]$ and $[z, w]$ are nonempty. Consider the question: what relationships must the numbers x, y, z, w satisfy to guarantee that $[x, y]$ and $[z, w]$ have nonempty intersection. The following statement gives an answer:

> **Proposition.** For all real numbers x, y, z, w satisfying $x \leq y$ and $z \leq w$, $[x, y] \cap [z, w] \neq \emptyset$ if and only if $x \leq w$ and $z \leq y$.

The proof of this statement illustrates many of the logical forms described above. In what follows there are comments included inside of brackets. These comments are not part of the proof, but are included to help you see the structure of the proof.

Proof. Let a, b, c, d to be arbitrary real numbers satisfying $a \leq b$ and $c \leq d$. [*Comment: The top-level structure of the proposition is a universal statement so we use the arbitrary value method.*]

Now we must show:

> $[a, b] \cap [c, d] \neq \emptyset$ if and only if $a \leq d$ and $c \leq b$.

To prove this, we must prove two things [*Comment: Using the logical form for proving "if and only if"*]:

1. If $[a, b] \cap [c, d] \neq \emptyset$ then $a \leq d$ and $c \leq b$.
2. If $a \leq d$ and $c \leq b$ then $[a, b] \cap [c, d] \neq \emptyset$.

We start by proving the first part. For this, we assume $[a,b] \cap [c,d] \neq \emptyset$ and must show $a \leq d$ and $c \leq b$. [*Comment: Using the logical form for "if–then". We must prove that both $a \leq d$ and $c \leq b$. are true.*]

The assumption $[a,b] \cap [c,d] \neq \emptyset$ tells us that there exists an object which we will call z that belongs to $[a,b] \cap [c,d]$. Since $z \in [a,b]$ we know that $a \leq z$ and since $z \in [c,d]$ we know that $z \leq d$ and combining these two inequalities gives $a \leq d$. Similarly since $z \in [c,d]$ we know that $c \leq z$ and since $z \in [a,b]$ we know that $z \leq b$ and combining these two inequalities gives $c \leq b$. Since both $a \leq d$ and $c \leq b$ this completes the first part.

Now let us prove the second part. Assume $a \leq d$ and $c \leq b$. We must show $[a,b] \cap [c,d] \neq \emptyset$.

To show that $[a,b] \cap [c,d] \neq \emptyset$ means we must show that there is an element in $[a,b] \cap [c,d] \neq \emptyset$. [*Comment: We must prove an existential statement, so we give instructions for selecting the desired element and prove that our instructions work. The instructions will depend on the unspecified numbes $a, b, c,$ and d. Also the instructions will depend on whether a is greater than c or not which means we will use cases.*]

Now, either $c \leq a$ or $a < c$, and we consider these two cases separately.

Case 1. Assume $c \leq a$. Since, by assumption, $a \leq d$ we have $a \in [c,d]$. Also since $a \leq a$ and $a \leq b$, we have $a \in [a,b]$. Therefore $a \in [a,b] \cap [c,d]$ and so $[a,b] \cap [c,d] \neq \emptyset$.

Case 2. Assume $a < c$. Since, by assumption, $c \leq b$ we have $c \in [a,b]$. Also since $c \leq c$ and $c \leq d$, we have $c \in [c,d]$. Therefore $c \in [a,b] \cap [c,d]$ and so $[a,b] \cap [c,d] \neq \emptyset$.

This completes the proof of the second part.

We therefore conclude that for all real numbers x, y, z, w satisfying $x < y$ and $z < w$, $[x,y] \cap [z,w] \neq \emptyset$ if and only if $x \leq w$ and $z \leq y$. $\square$