An Introduction to Writing Proofs

Prof. Susan Older

18 September 2012

Common Mathematics Terminology

Symbolic logic provides a backdrop for understanding how mathematicians (and related ilk) prove things, as well as the "parts of speech" of the language they use.

Common terms encountered in mathematics include:

- Definition
- Postulate (or axiom)
- Theorem
- Proof
- Proposition
- Lemma
- Corollary
- Claim
- Conjecture
- Counterexample

Definitions

A **definition** in mathematics is a statement that **stipulates** the meaning of a new term, symbol, or object:

- A definition **specifies precisely** what is meant by the term.
- A definition serves as the **sole authority** as to what that term means.
- Any subsequent statements regarding that term derive their meaning from the definition.

Examples of Definitions

Consider the following definitions:

Definition: An integer n is even if there exists an integer k such that $n = 2k$.

Definition: An integer n is odd if there exists an integer k such that $n = 2k + 1$.

What sorts of things can we conclude from these definitions?

- 24 is even, because $24 = 2 \cdot 12$ and 12 is an integer.
- 29 is odd, because $29 = 2 \cdot 14 + 1$ and 14 is an integer.
- Note that these definitions alone are **insufficient** for deducing that no number is both even and odd.
  (We would need to make use of additional properties of integers.)

A Last (?) Comment on Definitions

The standard form of a mathematics definition:

[Object] x is [defined term] if [defining property about x].

Mathematicians tend to write/say **if**, but they really mean **if and only if**.

Thus, the above definition really means

$$\forall x \in U, \ (D(x) \leftrightarrow P(x)),$$

where

$$\begin{aligned} U &= \text{set of objects under consideration} \\ D(x) &= \text{“}x\text{ is [defined term]”} \\ P(x) &= \text{“}x\text{ is [defining property about }x\text{”]} \end{aligned}$$

Example: $\forall n \in \mathbb{Z}, \ (even(n) \leftrightarrow \exists k \in \mathbb{Z} \text{ such that } n = 2k).$

Postulates (Axioms)

A **postulate** (also called an **axiom**) is a statement that is assumed true, without proof.

- Axioms are typically very basic, fundamental statements about the objects they describe.
- They serve as starting points from which other statements can be derived.
- A standard axiom about the natural numbers:

  If n is a natural number, then $n+1$ is also a natural number.

Theorems and Friends

A **theorem** is a statement that follows logically from axioms or other statements that have already been established.

- To be called a theorem, a statement must have a **proof**: that is, there must be a valid argument based on axioms, definitions, and proven theorems.
- A **lemma** is a theorem used to prove another theorem.
- **Proposition** is sometimes used to refer to a theorem that is considered less significant than other theorems.
- A **corollary** is a theorem that follows immediately from another theorem via a very short argument.

Claims, Conjectures, and Counterexamples

- A **claim** is a statement that we intend to prove.
- A **conjecture** is a statement that is thought to be true but has not been proved.
- A **counterexample** to a statement is a value that shows that statement to be false.
  - Consider a statement of the form $\forall x \in U,\ P(x)$.

    A counterexample is a value v such that $\neg P(v)$ is true.
  - Consider a statement of the form $\forall x \in U,\ (P(x) \to Q(x))$.

    A counterexample is a value v such that $\neg(P(v) \to Q(v))$ is true.

    Thus, it's a value v such that $P(v)$ is true and $Q(v)$ is false.

Mathematical Proofs

Mathematical proofs rely on the same underlying principles as formal proofs, with some important differences:

- The results tend to be expressed in paragraph form.
- They may not spell out all the details.

  Which details are included and which are omitted depend on the intended audience.
- Variables tend to be implicitly universally quantified, unless specified otherwise.

  The claim "If $A \cup B = \emptyset$, then $A = \emptyset$" really means:

  For all sets A and B, if $A \cup B = \emptyset$, then $A = \emptyset$.

In this class, we'll lean towards "more detail" rather than "less detail".

Overview of Proofs

Every proof has certain features:

- A collection of **hypotheses** (or **premises**) $H_1, H_2, \ldots, H_k$
- The desired **conclusion** C
- The need to show that, whenever **all** of the hypotheses are true, the conclusion is also true:

$$H_1 \wedge H_2 \wedge \cdots \wedge H_k \Rightarrow C$$

For now, we'll stick to **direct proofs**:

- Assume that $H_1 \wedge H_2 \wedge \cdots \wedge H_k$ is true (i.e., every hypothesis is true), and show that C is also true.

Later on, we'll consider some **indirect** styles of proofs.

Proving Existential Statements Directly

To prove a statement of the form

$$\exists x \in U \text{ such that } P(x),$$

it suffices to find a specific value $v \in U$ such that $P(v)$ is true.

Claim: There is a set X such that $\{1,2\} \subseteq X$ and $|\mathcal{P}(X)| > 10$.

Proof: Let $X = \{1,2,3,4\}$. Clearly $\{1,2\} \subseteq X$.

Recall that, for any set Y, $|\mathcal{P}(Y)| = 2^{|Y|}$. Because $|X| = 4$, we can see that

$$|\mathcal{P}(X)| = 2^{|X|} = 2^4 = 16 > 10.$$

Therefore, the claim is true.

Proving Universal Statements Directly (For Small Sets)

To prove a statement of the form

$$\forall x \in U,\ P(x) \qquad \text{(where } U \text{ is a smallish set)}$$

it suffices to show explicitly $P(v)$ is true for **every value v in U**.

Example

Claim: For all $w \in \{1,2,5\}$, $2w^2 \geq 2^w$.

Proof: Suppose $w \in \{1,2,5\}$. There are three possibilities:

- $w = 1$: Then $2w^2 = 2 \cdot 1^2 = 2 \geq 2^1 = 2^w$.
- $w = 2$: Then $2w^2 = 2 \cdot 2^2 = 2 \cdot 4 = 8 \geq 4 = 2^2 = 2^w$.
- $w = 5$: Then $2w^2 = 2 \cdot 5^2 = 2 \cdot 25 = 50 \geq 32 = 2^5 = 2^w$.

Therefore, for each $w \in \{1,2,5\}$, we have that $2 \cdot w^2 \geq 2^w$.

Proving Universal Statements Directly (Generalized)

To prove a statement of the form

$$\forall x \in U, \; P(x)$$

it suffices to select an **arbitrary value** $a \in U$ and show that $P(a)$ is true. (This is simply universal generalization!)

Example

Claim: For all $x \in \mathbb{R}$, $x^2 + 1 \geq 0$.

Proof: Let z be an arbitrary element of $\mathbb{R}$.
Because the square of any real number is nonnegative, we know $z^2 \geq 0$. Thus,

$$z^2 + 1 \geq 0 + 1 = 1 \geq 0.$$

Because z was arbitrary, the original claim is true.

Proving If-Then Statements Directly

To prove a statement of the form

$$\forall x \in U, \; (P(x) \rightarrow Q(x))$$

it suffices to select **arbitrary value** $a \in U$ and show $P(a) \rightarrow Q(a)$ is true.

How this is done in practice:

1. Consider an arbitrary $a \in U$.
2. Suppose that $P(a)$ is true.
3. Show that $Q(a)$ must also be true.

Sanity check: why does this work?

- If $P(a)$ is actually false, then $P(a) \rightarrow Q(a)$ is vacuously true, regardless of value of $Q(a)$.
- If $P(a)$ is actually true and we show $Q(a)$ is true, then $P(a) \rightarrow Q(a)$ is also true.

A Preview: Format of Proofs for CIS 275

We will be using the following format for all proofs in this course:

1. Explicitly specify what you're trying to prove.
   Proposition: For all integers n, if n is even, then $n + 1$ is odd.
2. Label the start of the proof, and indicate the method.
   Proof: (direct)
3. Explicitly state any initial assumptions.
   Let m be an integer, and suppose that m is even.
4. Explicitly state what you need to show, unwrapping the stopping condition as necessary.
   Need to show: $m + 1$ is odd. That is, there exists an integer k such that $m + 1 = 2k + 1$.
5. Fill in the gaps between steps 3 and 4 with the heart of the proof.
6. Explicitly wrap up the proof.
   Because m was arbitrary, the proposition is true.

A Basis for Some Sample Proofs

Recall the following two definitions:

Definition: An integer n is even if there exists an integer k such that $n = 2k$.

Definition: An integer n is odd if there exists an integer k such that $n = 2k + 1$.

We will also allow ourselves to use the following facts[1] about integers:

- If m and n are both integers, then $m + k$ is also an integer.
- If m and n are both integers, then $m \cdot k$ is also an integer.
- Every integer is either even or odd, but not both. That is, for all integers n,

$$n \text{ is odd} \equiv \neg(n \text{ is even})$$

[1] We use these as axioms, but a more rigorous treatment could prove them from other axioms.