Proof Shortcuts

MAKING THE TRANSITION FROM FORMAL TO INFORMAL PROOFS

Ken Monks
Dept of Mathematics
University of Scranton

In developing formal proofs in our math courses we quickly find that the perfect rigor they provide is quickly offset by the extreme length and tediousness of the proofs. The purpose of this sheet is to explain some of the shortcuts that mathematicians use in writing their proofs in order to shorten the proofs, make them more readable, and eliminate parts of the proof that are repetitive or uninteresting.

Let's begin with an example where we compare formal proofs, to what I will call "semi-formal" proofs. A semi-formal proof is a proof that is somewhere in between a completely formal proof (which only uses the rules of inference exactly as required) and a completely informal, word-wrapped, English proof that you find in many textbooks. This should help you to make the "transition" from formal to informal proofs and thus send you on your way to becoming true mathematicians.

First, consider the following FORMAL proof.

Thm A: $A \cap B \subseteq B$

Pf.

1.	$(A \cap B \subseteq B) \Leftrightarrow (\forall x, x \in A \cap B \Rightarrow x \in B)$	Def of $\subseteq$
2.	$(\forall x, x \in A \cap B \Rightarrow x \in B) \Rightarrow (A \cap B \subseteq B)$	$\Leftrightarrow -; 1$
3.	Let x be arbitrary.	—
4.	Assume $x \in A \cap B$	—
5.	$x \in A \cap B \Leftrightarrow x \in A$ and $x \in B$	Def of $\cap$
6.	$x \in A \cap B \Rightarrow x \in A$ and $x \in B$	$\Leftrightarrow -; 5$
7.	$x \in A$ and $x \in B$	$\Rightarrow -; 4, 6$
8.	$x \in B$	and $-; 7$
9.	$\leftarrow$	—
10.	$x \in A \cap B \Rightarrow x \in B$	$\Rightarrow +; 4, 8, 9$
11.	$(\forall x, x \in A \cap B \Rightarrow x \in B)$	$\forall +; 3, 10$
12.	$(A \cap B \subseteq B)$	$\Rightarrow -; 11, 2$

QED

Compare this with the semi-formal proof:

Thm A*: $A \cap B \subseteq B$

Pf.

1.	Let $x \in A \cap B$	—
2.	$x \in A$ and $x \in B$	Def of $\cap$; 1
3.	$x \in B$	and $-$; 2
4.	$(A \cap B \subseteq B)$	Def. of $\subseteq$; 1, 3

QED

In the second proof we have used many shortcuts and abbreviations to cut the proof down to the essential parts. Let's do another example before describing these shortcuts in more detail.

Thm B: $A \subseteq B \Rightarrow f(A) \subseteq f(B)$

Pf:

1.	Assume $A \subseteq B$	—
2.	$f(A) \subseteq f(B) \Leftrightarrow (\forall x, x \in f(A) \Rightarrow x \in f(B))$	Def of $\subseteq$
3.	$(\forall x, x \in f(A) \Rightarrow x \in f(B)) \Rightarrow f(A) \subseteq f(B)$	$\Rightarrow -$; 2
4.	Let b be arbitrary	—
5.	Assume $b \in f(A)$	—
6.	$f(A) = \{y \mid \exists x, x \in A \text{ and } y = f(x)\}$	Def of image
7.	$b \in \{y \mid \exists x, x \in A \text{ and } y = f(x)\}$	substitution; 6, 5
8.	$b \in \{y \mid \exists x, x \in A \text{ and } y = f(x)\} \Leftrightarrow (\exists x, x \in A \text{ and } b = f(x))$	Def of Set Builder
9.	$b \in \{y \mid \exists x, x \in A \text{ and } y = f(x)\} \Rightarrow (\exists x, x \in A \text{ and } b = f(x))$	$\Leftrightarrow -$; 8
10.	$\exists x, x \in A \text{ and } b = f(x)$	$\Rightarrow -$; 7, 9
11.	$a \in A$ and $b = f(a)$ for some constant a	$\exists -$; 10
12.	$a \in A$	and $-$; 12
13.	$A \subseteq B \Leftrightarrow (\forall x, x \in A \Rightarrow x \in B)$	Def of $\subseteq$
14.	$A \subseteq B \Rightarrow (\forall x, x \in A \Rightarrow x \in B)$	$\Leftrightarrow -$; 13
15.	$\forall x, x \in A \Rightarrow x \in B$	$\Rightarrow -$; 1, 14
16.	$a \in A \Rightarrow a \in B$	$\forall -$; 15
17.	$a \in B$	$\Rightarrow -$; 12, 16
18.	$b = f(A)$	and $-$; 11
19.	$a \in B$ and $b = f(A)$	and $+$; 17, 18
20.	$\exists x, x \in B \text{ and } b = f(x)$	$\exists +$; 19
21.	$b \in \{y \mid \exists x, x \in B \text{ and } y = f(x)\} \Leftrightarrow (\exists x, x \in B \text{ and } b = f(x))$	Def of Set Builder
22.	$(\exists x, x \in B \text{ and } b = f(x)) \Rightarrow b \in \{y \mid \exists x, x \in B \text{ and } y = f(x)\}$	$\Leftrightarrow -$; 21
23.	$b \in \{y \mid \exists x, x \in B \text{ and } y = f(x)\}$	$\Rightarrow -$; 23

24.	$f(B) = \{y \mid \exists x, x \in B \text{ and } y = f(x)\}$	Def of image
25.	$f(B) = f(B)$	reflexive
26.	$\{y \mid \exists x, x \in B \text{ and } y = f(x)\} = f(B)$	substitution;24, 25
27.	$b \in f(B)$	substitution;26, 23
28.	$\leftarrow$	—
29.	$b \in f(A) \Rightarrow b \in f(B)$	$\Rightarrow +; 5, 27, 28$
30.	$\forall x, x \in f(A) \Rightarrow x \in f(B)$	$\forall +; 4, 29$
31.	$f(A) \subseteq f(B)$	$\Rightarrow -; 30, 3$
32.	$\leftarrow$	—
33.	$A \subseteq B \Rightarrow f(A) \subseteq f(B)$	$\Rightarrow +; 1, 31, 32$

QED

compared to:

Thm B*: $A \subseteq B \Rightarrow f(A) \subseteq f(B)$
Pf:

1.	Assume $A \subseteq B$	—
2.	Let b be arbitrary	—
3.	Assume $b \in f(A)$	—
4.	$\exists x, x \in A \text{ and } b = f(x)$	Def of image;3
5.	$a \in A \text{ and } b = f(a)$ for some constant a	$\exists -; 4$
6.	$a \in A$	and $-$;
7.	$a \in B$	Def of $\subseteq; 1, 6$
8.	$a \in B \text{ and } b = f(a)$	and $+; 5, 7$
9.	$\exists x, x \in B \text{ and } b = f(x)$	$\exists +; 19$
10.	$b \in f(B)$	Def of image;9
11.	$\leftarrow$	—
12.	$b \in f(A) \Rightarrow b \in f(B)$	$\Rightarrow +; 3, 10, 11$
13.	$f(A) \subseteq f(B)$	Def of $\subseteq; 2, 12$
14.	$\leftarrow$	—
15.	$A \subseteq B \Rightarrow f(A) \subseteq f(B)$	$\Rightarrow +; 1, 13, 14$

QED

or using even more informality and shortcuts:

Thm B**: $A \subseteq B \Rightarrow f(A) \subseteq f(B)$
Pf:

1.	Let $A \subseteq B$	Given
2.	Let $b \in f(A)$	—
3.	$b = f(a)$ for some $a \in A$	Def of image;2

4. $a \in B$ Def of $\subseteq; 3, 1$
5. $b \in f(B)$ Def of image;$4, 3$
6. $f(A) \subseteq f(B)$ Def of $\subseteq; 2, 5$
QED

Proof Abbreviations and Shortcuts

With the above examples in mind, let's list some of the more common shortcuts and abbreviations used in semi-formal proofs.

I. Use the abbreviations: "Let $x \in A$", "$\forall x \in A, P(x)$", "$\exists x \in A, P(x)$","$\forall x_0, \ldots, x_n, P(x_0, \ldots, x_n)$", **and** "$\exists x_0, \ldots, x_n, P(x_0, \ldots, x_n)$"

We define "Let $x \in A$" to be an abbreviation for:

1. Let x be arbitrary.
2. Assume $x \in A$.

Notice that this destroys our careful indentations because there is a hidden assumption in the statement. Usually this is not a problem.

We also define "$\forall x \in A, P(x)$" as an abbreviation for "$\forall x, x \in A \Rightarrow P(x)$" and "$\exists x \in A, P(x)$" as an abbreviation for "$\exists x, x \in A$ and $P(x)$". These are used interchangeably in the proof, i.e. treated as if they are the same statement. Thus there is no need to convert form one form to the other.

Finally, we often combine multiple quantifiers into one by defining "$\forall x_0, \ldots, x_n, P(x_0, \ldots, x_n)$" as an abbreviation for "$\forall x_0 \forall x_1 \ldots \forall x_n, P(x_0, \ldots, x_n)$" and "$\exists x_0, \ldots, x_n, P(x_0, \ldots, x_n)$" as an abbreviation for "$\exists x_0 \exists x_1 \ldots \exists x_n, P(x_0, \ldots, x_n)$".

II. Use recipes that are derived from definitions and theorems rather than the definitions and theorems themselves.

We can always insert an entire theorem or definition as a line in our proof, but this is unwieldy in most cases. Instead, we use recipes (rules of inference) which are derived from the theorems and definitions. For example the definition of subset is

$$A \subseteq B \Leftrightarrow \forall x, x \in A \Rightarrow x \in B$$

but instead of using this directly in our proofs like this:

:
5. $x \in A$ for some reason
6. $A \subseteq B$ some other reason
7. $A \subseteq B \Leftrightarrow \forall x, x \in A \Rightarrow x \in B$ def of $\subseteq$
8. $A \subseteq B \Rightarrow \forall x, x \in A \Rightarrow x \in B$ $\Leftrightarrow -; 7$
9. $\forall x, x \in A \Rightarrow x \in B$ $\Rightarrow -; 6, 8$
10. $x \in A \Rightarrow x \in B$ $\forall -; 9$
11. $x \in B$ $\Rightarrow -; 5, 10$
:

we can use a recipe derived from the definition like this:

:
5. $x \in A$ for some reason

6. $A \subseteq B$ some other reason

7. $x \in B$ Def of $\subseteq; 5, 6$

:

III. Some Rules of Inference are often skipped or abbreviated

The following rules of inference are often skipped or abbreviated because they are "trivial":

a. and−

Example:

:

5. P and Q for some reason

6. $P \Rightarrow R$ some other reason

7. R $\Rightarrow -; 5, 6$

:

b. and+

Example:

:

5. P for some reason

6. Q some other reason

7. (P and Q) $\Rightarrow R$ yet another reason

8. R $\Rightarrow -; 5, 6, 7$

:

c. $\Leftrightarrow -$

Example:

:

5. $P \Leftrightarrow Q$ for some reason

6. P some other reason

7. Q $\Rightarrow -; 6, 5$

:

d. $\Leftrightarrow +$ and $\Rightarrow +$

In some cases we skip these steps as being obvious as in the following example.

Example:

Thm: $P \Leftrightarrow \sim\sim P$

Pf:

(⇒)

1. Assume P

: :

n. $\sim\sim P$

(⇐)

n+1. Assume $\sim\sim P$

: :

m. P

QED

Notice that the arrows ($\Rightarrow$) and ($\Leftarrow$) are used to make the proof more readable and indicate that the appropriate $\Rightarrow$ + and $\Leftrightarrow$ + rules are not being shown.

IV. Treat the following statement forms as if they are the same statement.

P or Q	is identified with	Q or P
P and Q	is identified with	Q and P
$P \Leftrightarrow Q$	is identified with	$Q \Leftrightarrow P$
$\sim\sim P$	is identified with	P
$x = y$	is identified with	$y = x$

a. Example:

:

5. P and Q — for some reason

6. $(Q$ and $P) \Rightarrow R$ — some other reason

7. R — $\Rightarrow -; 5, 6$

:

V. Use common tautologies freely

Tautology (or theorem)	Name
P or $\sim P$	Excluded Middle
$\sim(P$ and $Q) \Leftrightarrow (\sim P$ or $\sim Q)$	DeMorgan's Law
$\sim(P$ or $Q) \Leftrightarrow (\sim P$ and $\sim Q)$	DeMorgan's Law
$(P \Rightarrow Q) \Leftrightarrow (\sim Q \Rightarrow \sim P)$	Contrapositive
$(P$ and $Q)$ or $R \Leftrightarrow (P$ or $R)$ and $(Q$ or $R)$	Distributivity of and/or
$(P$ or $Q)$ and $R \Leftrightarrow (P$ and $R)$ or $(Q$ and $R)$	Distributivity of and/or
$(P \Rightarrow Q) \Leftrightarrow (\sim P$ or $Q)$	def of $\Rightarrow$
$\rightarrow\leftarrow \Rightarrow Q$	a contradiction implies anything
$(P$ or $Q)$ and $\sim P \Rightarrow Q$	special case of or-
$(\sim\forall x, P(x)) \Leftrightarrow \exists x, \sim P(x)$	DeMorgan's Law for quantifiers
$(\sim\exists x, P(x)) \Leftrightarrow \forall x, \sim P(x)$	DeMorgan's Law for quantifiers

Example:

:

5. $\sim(R$ and $\sim S)$ — for some reason

6. $\sim R$ or S — DeMorgan's Law;5

:

VI. Eliminate extra parentheses for associative logical operators

Use "P or Q or R" instead of "$(P \text{ or } Q)$ or R" or "P or $(Q \text{ or } R)$",

Use "P and Q and R" instead of "$(P \text{ and } Q)$ and R" or "P and $(Q \text{ and } R)$", etc.

VII. Use multiple rules of inference simultaneously where obvious

Example:

:

5. P and Q and R for some reason

6. Q and–;5

:

VIII. Use transitivity freely (chain notation)

Let $[r_1, r_2, \ldots, r_n]$ be a sequence of binary operators on a set A. We say such a sequence is *mutually transitive* if and only if for every $a, b, c \in A$, and for every $i, j \in \{1, 2, \ldots, n\}$, $a\, r_i\, b$ and $b\, r_j\, c \Rightarrow a\, r_n\, c$. Examples of mutually transitive operator sequences on the set of integers include: $[=]$, $[=, \leq]$, $[=, <]$, $[=, \leq, <]$, $[\geq, >]$, $\left[=, \underset{m}{\equiv}\right]$, and $[=, |]$. An example of a sequence of mutually transitive logical operators is $[\Leftrightarrow, \Rightarrow]$. Given such a sequence we can often shorten our proofs by using the *chain of operators* notation:

Chain of Operators Notation:

:

5. $x_1 \quad r_{i_1} \; x_2$

6. $\quad r_{i_2} \; x_3$

7. $\quad r_{i_3} \; x_4$

:

k. $\quad r_{i_{k-4}} \; x_{k-3}$

:

which is defined to be an abbreviation for:

:

5. $x_1 \quad r_{i_1} \; x_2$

6. $x_2 \quad r_{i_2} \; x_3$

7. $x_3 \quad r_{i_3} \; x_4$

:

k. $x_{k-4} r_{i_{k-4}} \; x_{k-3}$

:

Because the operators are mutually transitive we can conclude on line $k + 1$ that $x_1 \; r_n \; x_{k-3}$. This line can be omitted and the entire block of lines 5-k used as in its place in the proof.

Example:

:

5. $0 \quad \leq (a + 1)^2$

6. $\quad = a^2 + 2a + 1$

7. $< a^2 + 2a + 1 + 1$

8. $= a^2 + 2(a + 1)$

:

In this example, we see that $[=, \leq, <]$ is a mutually transitive sequence of operators, thus we can conclude from lines 5-8 that $0 < a^2 + 2(a + 1)$.

IX. Use "$\exists t, P(t)$" and "$P(t)$ for some t" interchangeably

This shortcut eliminates the use of the $\exists$ – rule by treating the bound variable in $\exists t, P(t)$ as the name of the constant produced by the $\exists$ – rule, or going directly to the conclusion of the $\exists$ – rule without stating the input to the rule. This reduces most applications of $\exists$ – rule from two lines to only one.

Example:

The following proof

:

5. $a \mid b$ for some reason

6. $\exists k \in \mathbb{Z}, ak = b$ def $\mid$; 5

7. $ak = b$ for some $k \in \mathbb{Z}$ $\exists -$; 6

8. $b + 1 = ak + 1$ substitution; 7, 8

:

can be abbreviated as:

:

5. $a \mid b$ for some reason

6. $\exists k \in \mathbb{Z}, ak = b$ def $\mid$; 5

7. $b + 1 = ak + 1$ substitution; 6, 7

:

where we are interpreting the bound variable k as automatically being declared as the global constant k, or we can go directly to the declaration:

:

5. $a \mid b$ for some reason

6. $ak = b$ for some $k \in \mathbb{Z}$ $\exists -$; 5

7. $b + 1 = ak + 1$ substitution; 6, 7

:

This last method is preferred because it avoids using a bound variable as a global one.

X. Skip writing the last line of the proof

If the last line of the proof is exactly the statement of the theorem you are trying to prove, and it clearly follows from your proof, there is no need to write it because the reader can see the statement of the Thm to see what your proof is trying to prove. The only exception would be if the last line has an unusual reason that should be explained to the reader. But most of the time the reason for the last line is either $\forall +$, $\Rightarrow +$, or proof by contradiction, so in these cases the last line isn't necessary.

XI. Use the shorthand notation $\{E(x_0, \ldots, x_n) : P(x_0, \ldots, x_n)\}$ for sets

In addition to set builder notation, $\{x : P(x)\}$ where P is a predicate, it is quite common practice in mathematics to write sets in the form $\{E(x_0, \ldots, x_n) : P(x_0, \ldots, x_n)\}$ where

$E(x_0,\ldots,x_n)$ is an expression containing the variables $x_0,\ldots,x_n$ and P is a predicate. This is defined to be a shorthand for

$$\{E(x_0,\ldots,x_n) : P(x_0,\ldots,x_n)\} = \{x : \exists x_0,\ldots,x_n, x = E(x_0,\ldots,x_n) \text{ and } P(x_0,\ldots,x_n)\}.$$

Example:

When we write $\mathbb{C} = \{a+bi : a,b \in \mathbb{R}\}$ this is an abbreviation for $\mathbb{C} = \{x : \exists a,b, x = a+bi \text{ and } a,b \in \mathbb{R}\}$ or equivalently $\mathbb{C} = \{x : \exists a,b \in \mathbb{R}, x = a+bi\}$. Thus if you need to pick an arbitrary element of $\mathbb{C}$ in your proof you should do it like this:

:

5. $\mathbb{C} = \{a+bi : a,b \in \mathbb{R}\}$ given

6. Let $z \in \mathbb{C}$ –

7. $z = a+bi$ for some $a,b \in \mathbb{R}$ def of $\mathbb{C}$;5,6

:

Example:

Suppose $I+J = \{a+b : a \in I \text{ and } b \in J\}$. Then this is an abbreviation for $\{x : \exists a \in I, \exists b \in J, x = a+b\}$. Thus to pick an arbitrary element of $I+J$ you should do it like this:

:

5. $I+J = \{a+b : a \in I \text{ and } b \in J\}$ given

6. Let $z \in I+J$ –

7. $z = a+b$ for some $a \in I, b \in J$ def of $I+J$;5,6

:

Example:

Suppose $S \subseteq R \times R$ by $S = \{(a,a) : a \in R\}$. Then this is an abbreviation for $\{x : \exists a \in R, x = (a,a)\}$. Thus to pick an arbitrary element of S you should do it like this:

:

5. $S = \{(a,a) : a \in R\}$ given

6. Let $z \in S$ –

7. $z = (a,a)$ for some $a \in R$ def of S;5,6

: