1 Proof Shortcuts

When writing formal proofs we quickly find that the perfect rigor they provide is quickly offset by the extreme length and tediousness of the proofs. Indeed, this aspect of formal proofs is often counter to our goal of elegant and effective exposition. So how can we retain the objective validity and rigor of a formal proof and make our proofs more elegant and expository at the same time?

One way is to use well-defined shortcuts that eliminate the tedious, obvious aspects of our proofs, while retaining the rigor and important concepts. In this document we list 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.

2 Shortcuts for Semi-formal Proofs

2.1 Use Theorems as Rules of Inference

Once we have proved a theorem we can use it to make new Rules of Inference. To use a theorem or definition as a rule of inference, we can just insert it as a line in our proof, and justify it with the name of the theorem and no premises. Doing so leaves the set of provable statements unaltered, i.e. no statement that could be proved with the new rules of inference could be proved without them, because we can always replace the new rule of inference with its proof.

So for example, if we prove the following simple theorem

**Theorem 1.** $P \Rightarrow P$

Then in a proof we can simply insert a line such as

12. $P \Rightarrow P$ by Theorem 1.

But we can do better.

A free variable that appears in a premise or conclusion of a Rule of Inference is called a metavariable. Metavarsibles in a rule can be replaced with any statement of the appropriate type before using the rule.

Similarly we can interpret the free variables in any Theorem as metavariables, and allow them to be replaced by an expression of the same type before inserting the theorem into our proof.

Interpreting Theorem 1 as a Rule of Inference in this way, we can thus insert a line in our proof like this

18. $\neg(Q \text{ or } R) \Rightarrow \neg(Q \text{ or } R)$ by Theorem 1.
This shortcut can also be applied to formal definitions, which can be thought of as a theorem whose proof is one line. These theorems can be used as a rule of inference in several ways.

### 2.2 Expand Theorems to Derive Rules of Inference

A more advanced way to avoid tedious repetitive steps of logic is to derive rules of inference from a theorem. Frequently a useful rule of inference is one that eliminates as many occurrences of quantifiers and logical operators as possible.

For example, if the theorem is an implication, i.e. of the form

**Theorem** (some famous implication). \( P \Rightarrow Q \)

then we can use it to justify the rule of inference \( P \vdash Q \). (Can you see why?) Then instead of using the theorem directly like this

\[
\text{some famous implication} \\
\text{Conclude: } P \Rightarrow Q
\]

we obtain a new rule

\[
\text{some famous implication} \\
\text{Show } P \\
\text{Conclude: } Q
\]

which is frequently more useful. Similarly if a theorem is a logical equivalence, i.e. has the form

**Theorem** (some famous equivalence). \( P \Leftrightarrow Q \)

then we can use it to justify two rules of inference, namely

\[
\text{some famous equivalence} \\
\text{Show: } P \\
\text{Conclude: } Q
\]
\[
\text{some famous equivalence} \\
\text{Show: } Q \\
\text{Conclude: } P
\]

We say such rules of inference are **derived** or **expanded** from the theorem.

There are other useful ways to expand rules of inference. It is frequently useful to make the following replacements.

<table>
<thead>
<tr>
<th>If the ROI has:</th>
<th>Replace that with:</th>
</tr>
</thead>
</table>
| Show \( P \) and \( Q \) | Show \( P \)  
| | Show \( Q \) |
| Show \( P \Rightarrow Q \) | Assume \( P \)  
| | Show \( Q \)  
| | ← |
2.3 Substitute Logically Equivalent Expressions

Whenever we have a theorem or definition that is an equivalence of the form $P \Leftrightarrow Q$, we can substitute occurrences of $P$ with $Q$ and vice versa whenever they appear as a subexpression in a statement in our proof. Equivalent statements have the same truth value, so replacing one with the other does not affect the validity of the statement where the substitution takes place.

For example, since we can prove that $\neg \neg P \Leftrightarrow P$, if we have a statement such as

$$\forall x, \exists y, \neg \neg \neg (y = x) \text{ and } f(y) = f(x)$$

We can immediately simplify this to

$$\forall x, \exists y, \neg (y = x) \text{ and } f(y) = f(x)$$

by substituting the subexpression $\neg (y = x)$ for the equivalent subexpression $\neg \neg \neg (y = x)$.
2.4 Use Famous Logic Theorems Freely

The following theorems about logic are quite well-known, and can usually be used in an expository proof without proving them or even justifying them with a reason (although you should in a formal or semi-formal proof). Since most of these are equivalences, they are frequently useful when combined with the previous shortcut.

<table>
<thead>
<tr>
<th>Theorems of Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>excluded middle</strong></td>
</tr>
</tbody>
</table>
| **double negative** | $\neg
\neg P \Leftrightarrow P$ |
| **idempotency** | $P$ and $P \Leftrightarrow P$ |
| **commutativity** | $P$ and $Q \Leftrightarrow Q$ and $P$ |
| **associativity** | $(P$ and $Q)$ and $R \Leftrightarrow P$ and $(Q$ and $R)$ |
| **distributivity** | $P$ and $(Q$ or $R) \Leftrightarrow (P$ and $Q)$ or $(P$ and $R)$ |
| **transitivity** | $(P \Rightarrow Q)$ and $(Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$ |
| **alpha substitution** | $(\forall x, P(x)) \Leftrightarrow (\forall y, P(y))$ |
| **alternate implies** | $(P \Rightarrow Q) \Leftrightarrow (\neg P$ or $Q)$ |
| **alternate or-** | $(P$ or $Q)$ and not $P \Rightarrow Q$ |
| **not implies** | not $(P \Rightarrow Q) \Leftrightarrow (P$ and not $Q)$ |
| **contrapositive** | $(P \Rightarrow Q) \Leftrightarrow (\neg Q$ or $\neg P)$ |
Theorems of Logic (cont.)

De Morgan's Law
\[ \neg (P \text{ and } Q) \iff \neg P \text{ or } \neg Q \]
\[ \neg (P \text{ or } Q) \iff \neg P \text{ and } \neg Q \]
\[ \neg \forall x, P(x) \iff \exists x, \neg P(x) \]
\[ \neg \exists x, P(x) \iff \forall x, \neg P(x) \]

contradiction
\[ \to \leftarrow \Rightarrow Q \]

alternate substitution
\[ x = y \text{ and } W \Rightarrow W \text{ with the nth free occurrence of } y \text{ replaced by } x. \]

alternate \( \exists ! \)
\[ (\exists ! x, W(x)) \iff \exists c, \forall z, W(z) \iff z = c \]

2.5 Identify Certain Statements

In some cases even using Shortcut 2.3 can still be too tedious. For example, if we have \( P \) and \( Q \) in our proof, but require \( Q \) and \( P \) as a premise, we might skip the substitution as a separate step, and instead do something like this:

\[
\begin{align*}
11. & \quad P \text{ and } Q \quad \text{for some reason} \\
12. & \quad (Q \text{ and } P) \Rightarrow R \quad \text{for some other reason} \\
13. & \quad R \quad \text{by } \Rightarrow - ; 11, 12 \\
\end{align*}
\]

Statements that typically can be identified without much trouble are given in the following table.

<table>
<thead>
<tr>
<th>the statement</th>
<th>can be identified with</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P \text{ and } Q )</td>
<td>( Q \text{ and } P )</td>
</tr>
<tr>
<td>( P \text{ or } Q )</td>
<td>( Q \text{ or } P )</td>
</tr>
<tr>
<td>( P \iff Q )</td>
<td>( Q \iff P )</td>
</tr>
<tr>
<td>( x = y )</td>
<td>( y = x )</td>
</tr>
<tr>
<td>( \neg \neg P )</td>
<td>( P )</td>
</tr>
</tbody>
</table>

2.6 Skip some logical rules of inference

While proof by contradiction, proof by cases, and other methods of proof are usually explicitly stated in a proof, some rules of inference are often skipped in an expository proof because they
are so obvious to the reader. This can be accomplished by allowing an expression to be used as a premise in place of some statement that can be logically derived from it.

For example, we usually skip the ‘ and +’ or ‘ and −’ rules by allowing $P$ and $Q$ to be used as a premise whenever $P$ or $Q$ are required, e.g.,

\[
\begin{align*}
11. & \quad P \text{ and } Q \quad \text{for some reason} \\
12. & \quad P \Rightarrow R \quad \text{for some other reason} \\
13. & \quad R \quad \text{by } \Rightarrow - \; ; \; 11,12
\end{align*}
\]

Similar shortcuts can be used to avoid ‘ and +’, e.g.,

\[
\begin{align*}
10. & \quad P \quad \text{for some reason} \\
11. & \quad Q \quad \text{for some other reason} \\
12. & \quad (P \text{ and } Q) \Rightarrow R \quad \text{for yet another reason} \\
13. & \quad R \quad \text{by } \Rightarrow - \; ; \; 10,11,12
\end{align*}
\]

Notice that in this case we can specify three premises even though the ‘$\Rightarrow+$’ only normally requires two premises. These examples can naturally be extended to expressions such as $P$ and $Q$ and $R$, and so on, even when using such an expression in place of, say, $Q$ would normally require more than one application of the ‘ and −’ rule.

A particularly common use of this shortcut is with the ‘$\iff+$’ rule. This is frequently abbreviated as follows.

Example 2. Suppose we have a theorem in this form (for some appropriate $P$ and $Q$).

Theorem 3. $P \iff Q$

Then we will frequently abbreviate the proof like this.

Proof

$(\Rightarrow)$

1. Assume $P$ -

\[
\begin{align*}
\vdots & \vdots \vdots \\
11. & \quad Q \quad \text{for some reason} \\
12. & \quad \leftarrow \quad - \\
(\iff)
\end{align*}
\]
13. Assume \( Q \) -  
\vdots \vdots \vdots  
33. \( P \) for some other reason  
34. \( \leftarrow \) -  
35. \( P \leftrightarrow Q \) by \( \leftrightarrow + \); 1, 11, 12, 13, 33, 34  
\( \Box \)

The notation (\( \Leftarrow \)) and (\( \Rightarrow \)) are just comments to indicate to the reader that we are proving an equivalence.

### 2.7 Sometimes skip the last line of the proof

Frequently when we write a proof is immediately follows the statement of the theorem being proved. Since the last line of the proof should be the statement of the theorem itself, it can frequently be omitted because the reader can refer to the theorem statement itself as long as the reason for the final statement would be obvious. (If not, then the reason should be stated even if it is in the form "Thus, the desired result follows by such-and-such a reason."

Some authors also omit any premises given in a theorem that is stated in the form \( P_1, \ldots, P_n \vdash Q \) for a similar reason. While this is common practice in mathematics, we don’t recommend it as it makes it more difficult to cite the premises when necessary, and can frequently make the proof more difficult for the reader to follow.

### 2.8 Eliminate extra parentheses for associative binary operators

A special case of Shortcut 2.5 is that we can eliminate extra parentheses for associative binary operators and allow the expression represent all possible ways of including the parentheses. For example, if we write

\[
P \text{ or } Q \text{ or } R \text{ or } S
\]

this expression can be identified with any of the expressions

\[
P \text{ or } (Q \text{ or } (R \text{ or } S))
\]

\[
P \text{ or } ((Q \text{ or } R) \text{ or } S)
\]

\[
(P \text{ or } Q) \text{ or } (R \text{ or } S)
\]

\[
(P \text{ or } (Q \text{ or } R)) \text{ or } S
\]

\[
((P \text{ or } Q) \text{ or } R) \text{ or } S
\]

### 2.9 Use the abbreviations "Let \( x \in A \)" , "\( \forall x \in A \)" , "\( \exists f : A \rightarrow B \)" , etc.

We define "Let \( x \in A \)" to be an abbreviation for:
Shortcuts and Recipes

Let $x$ be arbitrary.
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 \( P(x) \)". Once again, 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. We can think of this as declaring the type of the bound variable in the quantifier in each case.

Thus, in particular if you have the statement \( \exists x \in A, P(x) \) in your proof, you can apply the \( \exists - \) rule directly as shown.

\[
\begin{align*}
5. \quad & \exists x \in A, P(x) \quad \text{for some reason} \\
6. \quad & \text{For some } c \in A \\
7. \quad & P(c) \quad \text{by } \exists - ; 5
\end{align*}
\]

which in turn is equivalent to

\[
\begin{align*}
5. \quad & \exists x \in A, P(x) \quad \text{for some reason} \\
6. \quad & \text{For some } c \\
7. \quad & c \in A \text{ and } P(c) \quad \text{by } \exists - ; 5
\end{align*}
\]

Note that a line such as "For some $c \in A$ is both a statement and a constant declaration.

This idea can be extended to other predicates after the quantifier, i.e., "\( \forall Q(x), P(x) \)" as an abbreviation for "\( \forall x, Q(x) \Rightarrow P(x) \)" and "\( \exists Q(x), P(x) \)" as an abbreviation for "\( \exists x, Q(x) \) and \( P(x) \)". For example, we might say something like \( \forall f : A \rightarrow B, \forall x \in A, f(x) = 1 \). (For what set $B$ would this be true?)

Finally, we often combine multiple quantifiers into one by defining "\( \forall x_0, \ldots, x_n, \forall P(x_0, \ldots, x_n) \)" as an abbreviation for "\( \forall x_0, \forall x_1, \ldots \forall x_n, P(x_0, \ldots, x_n) \)" and "\( \exists x_0, \ldots, x_n, \exists P(x_0, \ldots, x_n) \)" as an abbreviation for "\( \exists x_0, \exists x_1, \ldots \exists x_n, P(x_0, \ldots, x_n) \)".
2.10 Use the shorthand notation \(\{E(x_0,\ldots,x_n) : P(x_0,\ldots,x_n)\}\)

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 free variables \(x_0,\ldots,x_n\) and \(P\) is a predicate. This is defined to be a shorthand for

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

Example 4. When we write

\[
C = \{a + bi : a, b \in \mathbb{R}\}
\]

this is an abbreviation for

\[
C = \{x : \exists a, b, x = a + bi \text{ and } a, b \in \mathbb{R}\}
\]

or equivalently

\[
C = \{x : \exists a, b \in \mathbb{R}, x = a + bi\}
\]

Thus, if you need to pick an arbitrary element of \(C\) in your proof you should do it like this:

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

6. Let \(z \in C\)

7. For some \(a, b \in \mathbb{R}\)

8. \(z = a + bi\) by the definition of \(C; 5, 6\)

2.11 Use Transitive Chains!

Let \(\langle r_1, r_2, \ldots, r_n \rangle\) 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 \(1 \leq i \leq j \leq n\),

\[
ar_i b \text{ and } br_j c \Rightarrow ar_j c
\]

and

\[
ar_i b \text{ and } br_i c \Rightarrow ar_j c
\]
Examples of mutually transitive operator sequences on the set of integers include: \(<=\), \(<=,\leq\), \(<=,\leq,\leq\), \(<=,\leq,<\), \(<=,\equiv\), \(<=,\leq\), \(<=,\equiv\) and \(<=,|\). An example of a sequence of mutually transitive logical operators is \(<\equiv,\Rightarrow\).

Given such a sequence we can often shorten our proofs by using the transitive chain notation

\[
\begin{align*}
x_1 & r_{i_1} x_2 \\
r_{i_2} & x_3 \\
r_{i_3} & x_4 \\
\vdots \\
r_{i_k} & x_{k+1}
\end{align*}
\]

which is defined to be an abbreviation for

\[
\begin{align*}
x_1 & r_{i_1} x_2 \\
x_2 & r_{i_2} x_3 \\
x_3 & r_{i_3} x_4 \\
\vdots \\
x_{k-1} & r_{i_k} x_{k+1}
\end{align*}
\]

Because the operators are mutually transitive we can use this entire block as a single premise to justify for any \(s, t\) such that \(1 \leq s \leq k\) and any \(s < t \leq k+1\) that \(x_i r_{\alpha} x_j\) where \(\alpha\) is the largest subscript among \(i_s, \ldots, i_{t-1}\). As a shortcut, any such deduction can be omitted and the entire block of lines used as in its place in the proof.

**Example 5.** In the following transitive chain, the sequence of operators, \(<=,\leq,<\), is mutually transitive.

\[
\begin{align*}
0 \leq (a + 1)^2 \\
&= a^2 + 2a + 1 \\
&< (a^2 + 2a + 1) + 1 \\
&= a^2 + 2(a + 1)
\end{align*}
\]

Thus, we can conclude from this transitive chain that \(0 < a^2 + 2(a + 1)\) (and other things, like \(0 \leq a^2 + 2a + 1\)).

### 2.12 Omit Most References to Premises and Line Labels

A somewhat sophisticated mathematical reader who is familiar with the premises needed to justify a statement with a given reason, can simply look for the required premises in the proof. Indeed, quite frequently one or more of the premises required immediately precede the line being justified in the proof.

We can thus remove some of the clutter by omitting references to premises that are obvious and easy to find. Similarly, this reduces or eliminates the need to label or number each line in the proof.
Mathematicians do label important statements and equations in their proofs and do refer to them when justifying statements. The rule of thumb to follow when deciding whether to explicitly label or reference a particular statement in your proof is whether it makes it improves the exposition for the reader. A non-obvious, or important statement that is referred to later on as a premise should still be labeled and referenced in order to make the proof easier to follow for the reader.

3 Problems

1. Use Shortcut 2.2 to derive useful rules of inference for each of the following definitions. Notice that you don’t actually need to understand what the definition says.

   (a) \[ f : G \rightarrow H \text{ and } f \text{ is a homomorphism } \iff \forall a, \forall b, a \in G \text{ and } b \in G \Rightarrow f(a \cdot b) = f(a) \cdot f(b) \]

   (b) \[ p \text{ is irreducible } \iff \forall g, (g \mid p) \Rightarrow g \text{ is a unit or } g \text{ is an associate of } p \]