Handout WP: Writing Proofs.

1. **Direct proof of an if-then statement.**
   Many theorems have the form “if \( p \) then \( q \)” where \( p, q \) are statements.
   (Note: \( p, q \) are often composed of other statements with and’s and or’s).
   A direct proof of \( p \implies q \) works like this:
   
   Assume: \( p \).
   To prove: \( q \).

2. **Proof by contrapositive.**
   The statement \( p \implies q \) is *logically equivalent to* (means: same truth-table)
   the statement \( \neg q \implies \neg p \). This means we can prove \( p \implies q \) like this:
   
   Assume: \( \neg q \).
   To prove: \( \neg p \).
   **Remark:** For any statement \( p \) you need to be able to compute \( \neg p \)
   (see the second handout "Quantifiers and Negation" for rules and examples
   on computing \( \neg p \) for any statement \( p \)).

3. **Proof by contradiction.**
   One way to prove a statement \( S \) is as follows:
   
   Assume: \( \neg S \).
   To prove: a contradiction.
   
   Proving a contradiction means proving something that is obviously wrong
   (e.g. \( x \neq x \), or the negation of a given/assumed/proved statement).

4. **Proving an if-then statement by contradiction.**
   If \( S \) is the statement \( p \implies q \) then \( \neg S \) is logically equivalent to \( p \land \neg q \).
   So a proof-by-contradiction for \( p \implies q \) works like this:
   
   Assume: \( p \) and \( \neg q \).
   To prove: a contradiction.

5. **Direct proof for a for-all statement.**
   If \( P(x) \) is a statement involving \( x \), to prove a statement like this \( \forall x \in A P(x) \)
   you write the following:
   
   Let \( x \in A \).
   To prove: \( P(x) \).
   **Explanation:** When you write "Let \( x \in A \)" then you are telling the
   reader that \( x \) is an element of \( A \), but you are not specifying *which* element
   of \( A \). That means that \( x \) could be any element of \( A \). Once you proved
   \( P(x) \) for such \( x \) then \( P(x) \) must be true for any element of \( A \).
   **What not to do:** Suppose \( f : S \to T \) and you want to prove \( \forall t \in T P(t) \).
   You should start with: "Let \( t \in T \)". But what if you this do instead:
   
   Some steps . . . take \( t = f(s) \) . . . some steps . . . hence \( P(t) \).
   Then you only proved \( P(t) \) for some, but not all, elements of \( T \).
6. **Direct proof for an exists statement.**
   If \( P(x) \) is a statement involving \( x \), to prove a statement like this \( \exists x \in A P(x) \) you write the following:
   Take \( x := \) [write down an expression].
   If it is obvious that the expression you wrote down meets the requirements \( x \in A \) and \( P(x) \) then the proof is now complete; you have a 1-line proof! (only non-obvious requirements need to be checked). If you wrote a lot of text but not this 1 line, then your proof is still not complete.

7. **Proving a for-all statement by contradiction.**
   If \( S \) is the statement \( \forall x \in A P(x) \) then \( \neg S \) is the statement \( \exists x \in A \neg P(x) \).
   So if we follow item 3 (i.e. prove \( S \) by assuming \( \neg S \) and then proving a contradiction) then the proof would start like this:
   Assume: \( x \) is an element of \( A \) and \( \neg P(x) \).
   To prove: a contradiction.

8. **Proving an exists-statement by contradiction.**
   If \( S \) is the statement \( \exists x \in A P(x) \) then \( \neg S \) is the statement \( \forall x \in A \neg P(x) \).
   Assume: \( \neg P(x) \) for every \( x \in A \).
   To prove: a contradiction.

9. **Proof by cases.**
   Suppose we need to prove some statement \( P(x) \) where \( x \) can only have a few possible values. In that case, we can write a separate proof for each possible value.
   **Example 1:** Suppose we have to prove \( P(x) \) but we know that \( x \) can only be \( u \) or \( v \) or \( w \). Then we write three proofs:
   Case 1: \( x = u \). Write a proof for \( P(u) \).
   Case 2: \( x = v \). Write a proof for \( P(v) \).
   Case 3: \( x = w \). Write a proof for \( P(w) \).
   **Example 2:** Suppose we have to prove a statement \( p \) but there is some other statement \( q \) such that we can easily find a proof for \( q \Rightarrow p \). Then we can do the following, we split the proof in two cases:
   Case 1: Assume \( q \) is true and prove \( p \) under that assumption.
   Case 2: Assume \( q \) is false now prove \( p \) under that assumption.
   These cases combined provide a complete proof for \( p \).

10. **Proving an and statement.**
    To prove \( p \land q \) write two separate proofs:
    To prove: \( p \)
    To prove: \( q \)
11. **Proving an iff statement** (iff = “if and only if”).
The statement $p \iff q$ is logically equivalent to $(p \implies q) \land (q \implies p)$. So to prove $p \iff q$ you have to write two proofs:

- To prove: $p \implies q$
- To prove: $q \implies p$

Proofs of “if and only if” statements in math books typically look like:

Assume $p$ . . . some math . . . hence $q$. For the converse . . .

Recall that $q \implies p$ is called the **converse** of $p \implies q$. Math books assume you know that “For the converse” means “To prove: $q \implies p$”.

12. **Proving an or statement.**
The statement $p \lor q$ means that at least one of $p$ or $q$ is true. But which one? That question makes it tricky to give a direct proof of $p \lor q$. But you can always replace a statement by a logically equivalent statement. We have several options:

1. $p \lor q$ is logically equivalent to $\neg p \implies q$.
2. $p \lor q$ is logically equivalent to $\neg q \implies p$.
3. $\neg(p \lor q)$ is logically equivalent to $\neg p \land \neg q$.

That gives us several ways to prove $p \lor q$.

- Method (3): Assume $\neg p$ and $\neg q$. To prove: a contradiction.

Which method is best? That depends on what you already know. Suppose for instance you see a theorem in the book of the form $\neg q \implies r$. In that case you want to try method (2) (assume $\neg q$) because then you can use the theorem to conclude $r$. Hopefully that brings you closer to goal $p$.

13. **Using an or statement.**
Suppose you want to prove $r$, and you are given $p \lor q$ which means that at least one of $p$ or $q$ is true. But which one? So we write two proofs:

- Assume $p$. To prove $r$.
- Assume $q$. To prove $r$.

The two proofs combined show that $p \lor q$ implies $r$.

This is the same as ”Proof by cases” from item 9; given $p \lor q$ you distinguish two cases: Case 1: assume $p$, to prove $r$. Case 2: assume $q$, to prove $r$.

14. If you want to **use a for-all statement** like $\forall x \in A P(x)$ to prove another statement, often the best strategy is to make a clever choice for one particular element of $A$, and then use the fact that $P$ is true for that element.

15. If you want to **use an exists statement** like $\exists x \in A P(x)$ to prove another statement, then you **may not choose** $x$. All you know is $x \in A$ and $P(x)$.