Proof Rules Handout
Theory and Practice of Algorithms
Drew Hilton
Duke ECE

This handout has two parts. First, we show you how to use each proof rule (introduction + elimination). Second, we give some common logical equivalences.

1 Proof rules

This section overviews each proof rule and how you use it. We do each rule written down in the style required for your homework, but with a focus just on that rule, rather than a holistic proof. Accordingly, we will write a "previously proven" with made up step numbers for whatever we must have proven before to use this rule.

1.1 And ($\wedge$)

And introduction:
Previously proven P (Step 1), Q (Step 2)
Usage:

3. $P \wedge Q$
   And-intro with 1 and 2.

You can use this with more than 2 clauses in the AND, you just need to have proven EACH part previously.
And elimination:
Previously proven $P \wedge Q$ (Step 1)
Usage (left):

2. P
   And-elim on 1.

Usage (right):

2. Q
   And-elim on 1.

You can also use this to pull out any term of a multi-clause AND. Note that if you think it helps add to clarity, you can specify which clause you are pulling out (e.g. And-elimination (left), or And-elimination(4th clause))

1.2 Or ($\vee$)

Or introduction:
Previously proven P (Step 1)
Usage(left):

2. $P \vee Q$
   Or-intro with 1

Usage(right):

2. $Q \vee P$
   Or-intro with 1

Note that you only need to have proven ONE clause of the OR. Also, you can use this with any number of clauses for the OR—you still need to have only proven one of them. If you think it adds to the clarity of the proof, note which one (as with AND). **Or elimination**:
Previously proven $P \vee Q$ (Step 1), $P \Rightarrow R$ (Step 2), $Q \Rightarrow R$ (Step 3)
Usage:

3. R
   Or-elim on 1, 2, and 3.

Note that you might see this called "constructive dilemma."

We are also happy with a slightly different form of this. Suppose you have only proven $P \vee Q \vee S$ (Step 1) already.

2. R
   By cases on 1.

   P ...

   Q ...

   S ...

Here each of the ...s either needs to be a claim (with justification) of R or a subproof yielding R. In each case, you can assume the corresponding proposition (P, Q, or S) for the case you are exploring.

Note that either form generalizes to any number of clauses in the OR.

1.3 Not ($\neg$)

Not introduction:
Not introduction is proof by contradiction. It generally looks like this

1. $\neg P$
   By contradiction: assume P and...
   1.1. Q
   1.2. $\neg Q$
   1.3. False
   Contradiction between 1.1 and 1.2

Note that whatever you are proving by contradiction, you assume the opposite. To prove $\neg P$, you assume P. You can also prove P by assuming $\neg P$ (technically, you are proving $\neg\neg P$ by contradiction, then doing double-negation elimination on it, but we don't require you to show that step). Your sub-proof must conclude False. **Not elimination**:
Previously proven: $\neg\neg P$ (Step 1)

2. P
   By not-elim on 1

Note that you unlike most rules, we will allow you to (1) remove double negations implicitly and (2) remove them internally to other things (all other rules can only be applied to at the "top" of a proposition).

1.4 Implication ($\Rightarrow$)

Implication introduction:

1. $P \Rightarrow Q$ Assume P and..
   - a sub proof concluding Q

Implication elimination:
Previously proven $P \Rightarrow Q$ (Step 1) and P (Step 2)

3. Q
   Implication-elim on 1 and 2

Note that the formal name for this rule is "modus ponens." Accordingly, we are happy for you to abbreviate it MP:

3. Q
   MP: on 1 and 2

1.5 Iff ($\Leftrightarrow$)

Iff introduction:
Previously proven: $P \Rightarrow Q$ (Step 1), $Q \Rightarrow P$ (Step 2)

3. $P \Leftrightarrow Q$
   Iff-intro on 1 and 2

Iff elimination: Previously proven: $P \Leftrightarrow Q$ (Step 1)
Usage (left):

2. $P \Rightarrow Q$
   Iff-elim on 1

Usage (right):

2. $Q \Rightarrow R$
   Iff-elim on 1

Note that if it helps clarity, you can specify Iff-elim(left) or Iff-elim(right).

1.6 Exists ($\exists$)

Exists introduction: Previously proven $P(x)$ (Step 1)
Usage:

2. $\exists y.P(y)$
   Exists-intro on 1 with witness $y = x$

Exists elimination: Previously proven $existsx.P(x)$ (Step 1)
Usage:

2. Q
   Exists-elim on 1 ($P(y)$) in...
   - (sub-proof concluding Q)

Note that y cannot be *free* in Q.

1.7 Forall ($\forall$)

Forall introduction: pick-any:
Usage:

1. $\forall x \in$ Things.$P(x)$
   Pick any thing a and...
   - (subproof concluding $P(x)$)

Note that you must not know anything about x—that is, x cannot appear free in any conclusion or assumption that is "available" to you. If x does, pick a different variable. $\forall x.P(x)$ and $\forall y.P(y)$ are logically equivalent. **Forall introduction: weak induction**:
Usage:

1. $\forall x \in \mathbb{N}.P(x)$
   By weak-induction on x:

Base: 0.
   Goal: $P(0)$
   Proof: (sub-proof proving $P(0)$)

Ind.
   IH: $P(n)$
   Goal: $P(n+1)$
   Proof: (sub-proof that assumes IH, and proves $P(n+1)$)

It is legal to have more than one base case (Base: 0, Base :1, ...) which changes your inductive case. If you B base cases, you are trying to prove $P(n+B)$, but you also have B inductive hypotheses. For example:

1. $\forall x \in \mathbb{N}.P(x)$
   By weak-induction on x:

Base: 0.
Goal: $P(0)$
Proof: (sub-proof proving $P(0)$)

Base: 1.
Goal: $P(1)$
Proof: (sub-proof proving $P(1)$)

Base: 2.
Goal: $P(0)$
Proof: (sub-proof proving $P(0)$)

Ind.
IH0: $P(n)$
IH1: $P(n+1)$
IH2: $P(n+2)$
Goal: $P(n+3)$
Proof: (sub-proof that assumes IH0, IH1, and IH2, and proves $P(n+3)$)

Forall introduction: strong induction:
Usage:

- $\forall x \in \mathbb{N}.P(x)$
  By strong induction on x

Base 0.
Goal: $P(0)$
Proof: (sub-proof proving $P(0)$)

Ind.
IH: $\forall n \in \mathbb{N}.n < x \Rightarrow P(n)$
Goal: $P(x)$
Proof: (sub-proof that assumes IH and proves $P(x)$)

Forall elimination: Previously proven: $\forall x.P(x)$ (Step 1)
Usage:

2. $P(y)$
   Forall-elim on 1 with $x = y$

Note that this rule is also called "universal specialization", so we are happy for you to abbreviate it "Uspec" like this:

2. $P(y)$
   Uspec on 1 with $x = y$

2 Logical equivalences

The following are useful logical equivalences:

Demorgan's Laws.

- $P \vee Q$ is equivalent to $\neg(\neg P \wedge \neg Q)$
- $P \wedge Q$ is equivalent to $\neg(\neg P \vee \neg Q)$

Quantifier equivalence.

- $\forall x.P(x)$ is equivalent to $\neg\exists x.\neg P(x)$
- $\exists x.P(x)$ is equivalent to $\neg\forall x.\neg P(x)$

Meaning of implication. $P \Rightarrow Q$ is equivalent to $\neg P \vee Q$

Contrapositive. $P \Rightarrow Q$ is equivalent to $\neg Q \Rightarrow \neg P$

Distributive Laws.

- $P \vee (Q \wedge R)$ is equivalent to $(P \vee Q) \wedge (P \vee R)$
- $P \wedge (Q \vee R)$ is equivalent to $(P \wedge Q) \vee (P \wedge R)$