Proof Techniques

By
Chuck Cusack

These notes are loosely based on material from section 3.1 of *Discrete Structures and its Applications*, 4th Edition

1

Why Proofs?

- Writing proofs is not most student's favorite activity.
- To make matters worse, most students do not understand why it is important to prove things.
- Here are just a few reasons proofs are useful.
  - Given a segment of code, it can be very beneficial to know that it does what you think it does. Then if you have a problem, you can be absolutely sure that the problem is not with that segment of code.
  - When you are solving problems, you usually make assumptions. It may be useful and/or necessary to make sure the assumptions are actually valid, which may involve proving something.

2

Theorems

- A theorem is a statement that can be shown to be true.
- By "shown to be true," we mean that a proof can be constructed that verifies the statement.
- An axiom or postulate is a statement which we either know or assume is true.
- Axioms and postulates are usually called assumptions since they are the things we assume are true.
- Theorems generally contains a list of assumptions, p_1, p_2, …, p_n, and the conclusion that can be drawn from them, q.

Example Theorem: If $x>0$ and $y>0$, then $x+y>0$.

- The validity of a proof is based on the validity of the axioms or postulates, and the correctness of each step of the proof.

3

Other True Things

- Not every statement that is true is called a theorem.
- Other terms you may see include
  - Lemma (usually a statement that is proved only because you want to prove something else).
  - Corollary (usually a statement that is easily proven given a previously proved theorem, lemma, etc.)
  - Proposition
- Sometimes, no fancy name is given at all.
- In fact, the examples in these notes are not called anything special.
- There is no special significance to calling something a theorem, except that it means it is true, although the term is often reserves for more significant true statements.
- You may also see the term conjecture. This is a statement that is believed to be true, but for which no proof is known.

4

How To Construct A Proof

All proofs are constructed in essentially the same way:

- You start with a statement of the problem, which will state the assumptions, p_1, p_2, …, p_n, and the conclusion that can be drawn from them, q.

  Example: Show that if $x>0$ and $y>0$, then $x+y>0$.
- You then show that $p_1 \wedge p_2 \wedge \ldots \wedge p_n \rightarrow q$.
- This usually involves proving intermediate conclusions by applying a rule of inference or other correct proof technique to one or more of the assumptions and previous intermediate conclusions, until the final conclusion can be drawn.
- In the beginning, you should practice explicitly justifying every step of the proof.

5

Proper Proof Technique

- As stated previously, each step of a proof must be properly justified.
- What is a proper justification?
- It is difficult to give a complete answer, but the following are all valid:
  - Rules of inference (more in the next few slides)
  - Applying a definition
  - Applying algebra
  - Substituting one thing for an equivalent thing
- As you are learning to construct proofs, you should be very careful to make sure that the techniques you use are valid.
- If you are not sure if a step in a proof is valid, do not use it.

6

Rules of Inference

- A rule of inference allows us to use one or more things we know are true to prove that another thing is also true.
- Since this is probably still unclear, an example is in order.

Example:

- Consider the proposition (p∧(p→q))→q.
- You can easily verify that this is a tautology.
- If you think about what this means, it is also not hard to convince yourself that this should be true:

p	q	p→q	p∧(p→q)	(p∧(p→q))→q
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

“If we know that p is true, and we know that p is true implies q is true, then it must be the case that q is true.”

- This tautology yields a rule of inference.

7

Rules of Inference II

Example continued:

- The tautology (p∧(p→q))→q is the basis of the rule of inference known as modus ponens.
- The rule can be written as:
- What this means is if we know that p is true, and we know that p→q is true, then we can say (with confidence) that q is true.

p
p→q
∴q

Example use of example inference:

- It is true that if a student scores an average of at least 93% (p), they will get an A in this class (q).
- What can you say about a student who has an average of at least 93% (p)?

8

And the rest…

- We will take a look at 8 of the most commonly used rules of inference.
- Each of them is based on a tautology of the general form

p→q

- This makes sense, because in a proof, we want to prove one thing (q) based on one or more things (p) we already know to be true.
- We leave it to the reader to verify that each proposition is in fact a tautology.

9

Addition

- The tautology p→(p∨q) is the basis for the rule known as addition.
- It can be phrased in English as “If we know that p is true, then we know that either p is true or q is true.”
- The rule can be written as:

p
∴p∨q

Example:

- Since it is true that you came to class today, then either you came to class today, or you went to the park today.

10

Simplification

- The tautology (p∧q)→p is the basis for the rule known as simplification.
- It can be phrased in English as “If we know that p and q are both true, then we know that p is true.”
- The rule can be written as:

p∧q
∴p

Problem:

- Prove that if $0 < x < 10$, then $x \geq 0$.

Proof:

- $0 < x < 10$ is the same as $x > 0$ and $x < 10$.
- $x > 0$ and $x < 10$ imply that $x > 0$ by simplification.
- $x > 0$ implies that $x > 0$ or $x = 0$ by addition.
- $x > 0$ or $x = 0$ is the same as $x \geq 0$.

11

Conjunction

- The tautology ((p)∧(q))→ (p∧q) is the basis for the rule known as conjunction.
- It can be phrased in English as “If we know that p is true, and we know that q is true, then we know that p∧q is true.”
- The rule can be written as:

p
q
∴ p∧q

- Generally we apply this rule without justification, since it is pretty straightforward.

12

Modus Ponens

- As we have already seen, the tautology $[p\wedge(p\rightarrow q)]\rightarrow q$ is the basis of the rule of inference known as modus ponens.
- In English, the rule states that "If p is true, and p implies q, then q is true."
- The rule can be written as:

p
$p\rightarrow q$
$\therefore q$

Problem:

- You know that if you study, you will pass. Since you are in my class, it is given that you will study and you will read your textbook. Prove that you will pass.

Proof:

- Let p="you will study," q="you will pass," and r="you will read your textbook." Then we know that $p\rightarrow q$ and $p\wedge r$.
- By simplification, $p\wedge r$ implies p.
- Since we know p and $p\rightarrow q$, by modus ponens we know q.
- Thus, you will pass.

Modus Tollens

- The tautology $[\neg q\wedge(p\rightarrow q)]\rightarrow\neg p$ is the basis of the rule of inference known as modus tollens.
- In English, the rule states that "If p implies q, and q is false, then p is false," which makes sense.
- The rule can be written as:

$\neg q$
$p\rightarrow q$
$\therefore\neg p$

Problem:

- Everyone knows that dogs are stupid. You aren't stupid. Can you prove that you are not a dog?

Proof:

- A simple application of modus tollens tells you you are not a dog.

Hypothetical Syllogism

- The tautology $[(p\rightarrow q)\wedge(q\rightarrow r)]\rightarrow(p\rightarrow r)$ is the basis of the rule of inference known as hypothetical syllogism.
- In English, the rule states that "If p implies q, and q implies r, then p implies r."
- The rule can be written as:

$p\rightarrow q$
$q\rightarrow r$
$\therefore p\rightarrow r$

Problem:

- If you drop your laptop from the top of the building, you will lose everything on the hard drive. If you walk on top of the building during a rain storm, you will drop your laptop.
- What can you conclude?

Proof:

- By hypothetical syllogism, you know that if you walk on top of the building during a rainstorm, you will lose everything on the hard drive.

Disjunctive Syllogism

- The tautology $[(p\vee q)\wedge\neg p]\rightarrow q$ is the basis of the rule of inference known as disjunctive syllogism.
- In English, the rule states that "If p or q is true, and p is not true, then q is true."
- The rule can be written as:

$p\vee q$
$\neg p$
$\therefore q$

Problem:

- You either learned the material from this course, or you tricked me, if you pass. You did not trick me. I passed you. Prove that you learned the material from the course.

Proof:

- Since you passed, the first sentence and modus ponens implies you either learned the material from the course, or you tricked me.
- Since you did not trick me, disjunctive syllogism allows us to conclude that you learned the material from the course.

Contrapositive

- The tautology $(p\rightarrow q)\rightarrow(\neg q\rightarrow\neg p)$ is the basis for the rule known as contrapositive.
- It can be phrased in English as "If p implies q, then q false implies that p is false."
- The rule can be written as:

$p\rightarrow q$
$\therefore\neg q\rightarrow\neg p$

Problem:

- If you are enrolled in this course, then I will give you a grade at the end of the semester. If you are not enrolled in this course, you are not here today. What can you conclude?

Proof:

- By contrapositive, the second sentence implies that if you are here today, you are enrolled in this course.
- Applying hypothetical syllogism to the above sentence and the first sentence above, you can conclude that if you are here today, I will give you a grade at the end of the semester.

Rules of Inference Summary

Rules of Inference	
Tautology	Rule
$p\rightarrow(p\vee q)$	Addition
$(p\wedge q)\rightarrow p$	Simplification
$((p)\wedge(q))\rightarrow(p\wedge q)$	Conjunction
$[p\wedge(p\rightarrow q)]\rightarrow q$	Modus Ponens
$[\neg q\wedge(p\rightarrow q)]\rightarrow\neg p$	Modus Tollens
$[(p\rightarrow q)\wedge(q\rightarrow r)]\rightarrow(p\rightarrow r)$	Hypothetical Syllogism
$[(p\vee q)\wedge\neg p]\rightarrow q$	Disjunctive Syllogism
$(p\rightarrow q)\rightarrow(\neg q\rightarrow\neg p)$	Contrapositive

Example Proof #1

Problem

- The statements $p \rightarrow q$, $r \rightarrow s$, and $r \vee p$ are true, and q is false.
- Show that s is true.

Proof

- Since $p \rightarrow q$ and $\neg q$ are true, $\neg p$ is true by modus tollens.
- Since $r \vee p$ and $\neg p$ are true, r is true by disjunctive syllogism.
- Since $r \rightarrow s$ and r are true, s is true by modus ponens.

19

Example Proof #2

Problem

- Show that the sum of two odd integers is even.

Proof

- Let x and y be the two odd integers (the assumption)
- Since they are odd, we can write $x = 2a + 1$ and $y = 2b + 1$ for some integers a and b (definition)
- Then

  $x + y = 2a + 1 + 2b + 1$ (substitution)

  $= 2a + 2b + 2$ (algebra)

  $= 2(a + b + 1)$ (algebra)
- $2(a + b + 1)$ is even (definition)
- Therefore, $x+y$ is even.

20

Example Proof #3

Problem

- Show that if an integer x is odd then x^2 is odd.

Proof

- If x is odd then $x=2k + 1$ for some integer k. (definition)
- Then $x^2=(2k + 1)^2$ (substitution)

  $=4k^2 + 4k + 1$ (algebra)

  $=2l + 1$ (substituting $l=2k^2+2k$)
- Therefore x^2 is odd. (definition)

21

False Proofs

There are 3 common mistakes in constructing proofs

1. Fallacy of affirming the conclusion, based on the proposition $[q \wedge (p \rightarrow q)] \rightarrow p$, which is NOT a tautology.
2. Fallacy of denying the hypothesis, based on the proposition $[\neg p \wedge (p \rightarrow q)] \rightarrow \neg q$, which is NOT a tautology.
3. Circular reasoning, in which you assume the statement you are trying to prove is true.

Since I don't want to encourage use of these for obvious reasons, I will not give an example.

22

If and Only If (IFF)

- Some problems actually involve proving that p is true if and only if q is true, instead of simply p implies q.
- Usually, these proofs are simply broken into two parts: proving p implies q, and proving q implies p.
- In some cases, the proof can "work both ways" so that only one part is necessary.

Example:

- Show that an integer x is odd if and only if x^2+2x+1 is even.

Proof:

- x is odd iff $x = 2k + 1$ for some integer k (definition)

  iff $x+1 = 2k + 2$ for some integer k (algebra)

  iff $x+1 = 2m$ for some integer m (algebra)

  iff $x+1$ is even (definition)

  iff $(x+1)^2$ is even (x even iff x^2 even)

  iff x^2+2x+1 is even (algebra)
- Each step was reversible, so we have shown both ways.

23

Types of proofs

There are many different types of proofs.

- Trivial proof
- Vacuous proof
- Direct proof
- Indirect proof
- Proof by contradiction
- Proof by cases

We briefly describe and give an example of each

24

Trivial Proof

- A trivial proof is a proof of a statement of the form $p \to q$ which proves *q* without using *p*.
- **Example:** Prove that if x>0, then $(x+1)^2 - 2x > x^2$.
- **Proof:** It is easy to see that

$$
\begin{aligned}
(x+1)^2 - 2x &= (x^2 + 2x + 1) - 2x \\
&= x^2+1 \\
&> x^2.
\end{aligned}
$$

- Notice that I never used the fact that x>0 in the proof.

25

Vacuous Proof

- If *p* is false, then $p \to q$ is true regardless of the value of *q*.
- Thus, if *p* is false, then $p \to q$ is true trivially.
- A vacuous proof is a proof of a statement of the form $p \to q$ which shows that *p* is false.
- **Example:** Prove that if 1+1=1, then I am the Pope.
- **Proof:** Since $1+1 \neq 1$, the premise is false. Therefore the statement "if 1+1=1, then I am the Pope" is true.

26

Direct Proof

- A direct proof is a proof of a statement of the form $p \to q$ which assumes *p* and proves *q*.
- Most of the proofs we have seen so far are direct proofs.
- **Example:** Prove that if $x \geq 4$, then $x^2 > 15$.
- **Proof:** Let $x \geq 4$. Then we can write x = y + 3, for some $y \geq 1$. Thus,

$$
\begin{aligned}
x^2 &= (y+3)^2 \\
&= y^2 + 6y + 9 \\
&> 6y + 9 \\
&\geq 6 + 9 \\
&= 15.
\end{aligned}
$$

27

Indirect Proof

- Since $p \to q$ is equivalent to the contrapositive $\neg q \to \neg p$, a proof of the latter is a proof of the former.
- An indirect proof is a proof of a statement of the form $p \to q$ which proves $\neg q \to \neg p$ instead.

Example:

- Prove that if $x^3 < 0$, then $x < 0$.

Proof:

- This statement is equivalent to "if $x \geq 0$, then $x^3 \geq 0$."
- If x=0, clearly $x^3 = 0 \geq 0$.
- If x>0, then $x^2 > 0$, so

$$
\begin{aligned}
x^3 \geq 0 &\Leftrightarrow x^3/x^2 \geq 0/x^2 && \text{(algebra)} \\
&\Leftrightarrow x \geq 0. && \text{(algebra)}
\end{aligned}
$$

28

(Recall that we can multiply or divide both sides of an inequality by any positive number.)

Proof by Contradiction

- If you want to prove that a statement *p* is true, you can assume that *p* is false, and develop a contradiction.
- That is, demonstrate that if you assume *p* is false, then you can prove a statement that is known to be false.
- In logic terms, you pick a statement *r*, and show that $\neg p \to (r \wedge \neg r)$ is true. Since this is not possible, it must be that *p* is true.
- A proof of this type is called a proof by contradiction for hopefully obvious reasons.

29

Example Proof by Contradiction

Problem: Prove that the product of a nonzero rational number and an irrational number is irrational.

Proof:

- Assume that the product of a rational and an irrational number is rational (the negation of what we want to prove.)
- Then we can express this as $xw=y$, where *x* and *y* are rational, and *w* is irrational.
- Thus, we can write $x=a/b$ and $y=c/d$, for some integers *a*, *b*, *c*, and *d*.
- Then $xw=y$ is equivalent to $w = y/x = (c/d)/(a/b) = bc/ad = e/f$, where $e=bc$ and $f=ad$, which are both integers.
- Since *e* and *f* are both integers, *w* is rational. But *w* is irrational. This is a contradiction.
- Therefore the product of a rational and irrational is irrational.

30

Proof by Cases

- Sometimes it is easier to prove a theorem by breaking it into several cases.
- This is best seen in an example.
- **Example:** Prove that $x^2>0$ for any $x\neq 0$.
- **Proof:**
- If x>0 (case 1), then we can multiply both sides of x>0 by x, giving $x^2>0$.
- If x<0 (case 2), we can write y=-x, where y>0.
- Then $x^2 = (-y)^2 = ((-1)y)^2 = (-1)^2y^2 = 1y^2 = y^2>0$, since y>0 (see case 1).
- Therefore if $x\neq 0$, then $x^2>0$.

31

Proofs with Quantifiers

- When statements in proofs involve quantifiers, we need a way to deal with them.
- The following rules of inference are useful.
- For each, the universe of discourse is **U**.

Rules of Inference for Quantifiers	
$\forall x\, P(x)$ $\therefore P(c)$ if $c\in U$	Universal instantiation
$P(c)$ for arbitrary $c\in U$ $\therefore \forall x\, P(x)$	Universal generalization
$\exists x\, P(x)$ $\therefore P(c)$ for some $c\in U$	Existential instantiation
$P(c)$ for some $c\in U$ $\therefore \exists x\, P(x)$	Existential generalization

32

Example Proof with Quantifier

- Consider the statements:
  - "All hummingbirds are richly colored"
  - "No large birds live on honey"
  - "Birds that do not live on honey are dull in color"
- Prove the statement
  - "Hummingbirds are small."

Proof:

- We start by letting
  - P(*x*)="*x* is a hummingbird"
  - Q(*x*)="*x* is large"
  - R(*x*)="*x* lives on honey"
  - S(*x*)="*x* is richly colored"

Based on Example 21 from section 1.3 of *Discrete Structures and its Applications*, 4th Edition 33

Example Part 2

Statements:

"All hummingbirds are richly colored"
"No large birds live on honey"
"Birds that do not live on honey are dull in color"

Conclusion:

"Hummingbirds are small."

Definitions:

P(*x*)="*x* is a hummingbird"
Q(*x*)="*x* is large"
R(*x*)="*x* lives on honey"
S(*x*)="*x* is richly colored"

- We can express the statements as
  - $\forall x[P(x)\rightarrow S(x)]$
  - $\neg\exists x[Q(x)\wedge R(x)]$
  - $\forall x[\neg R(x)\rightarrow \neg S(x)]$
- We can express the conclusion as
  - $\forall x[P(x)\rightarrow \neg Q(x)]$
- We need to show the conclusion given the three statements.

34

Example Part 3

Statements:
$\forall x[P(x)\rightarrow S(x)]$
$\neg\exists x[Q(x)\wedge R(x)]$
$\forall x[\neg R(x)\rightarrow \neg S(x)]$

Conclusion:
$\forall x[P(x)\rightarrow \neg Q(x)]$

- First, notice that
  - $\neg\exists x[Q(x)\wedge R(x)]$
  - $\Leftrightarrow\forall x\neg[Q(x)\wedge R(x)]$
  - $\Leftrightarrow\forall x[\neg Q(x)\vee\neg R(x)]$
- By universal instantiation, we know that given an arbitrary element $x\in U$, each of the following statements is true:
  - $P(x)\rightarrow S(x)$
  - $\neg Q(x)\vee\neg R(x)$
  - $\neg R(x)\rightarrow \neg S(x)$
- Since $\neg R(x)\rightarrow\neg S(x)$ is true, the contrapositive is true:
  - $S(x)\rightarrow R(x)$

35

Example Part 4

What we know:
$P(x)\rightarrow S(x)$
$\neg Q(x)\vee\neg R(x)$
$\neg R(x)\rightarrow \neg S(x)$
$S(x)\rightarrow R(x)$

Conclusion:
$\forall x[P(x)\rightarrow \neg Q(x)]$

- Since $P(x)\rightarrow S(x)$ and $S(x)\rightarrow R(x)$, hypothetical syllogism gives us
  - $P(x)\rightarrow R(x)$
- Since $\neg Q(x)\vee\neg R(x)$ is true, the implication law implies
  - $R(x) \rightarrow\neg Q(x)$
- Since $P(x)\rightarrow R(x)$ and $R(x)\rightarrow \neg Q(x)$, hypothetical syllogism allows us to say
  - $P(x)\rightarrow \neg Q(x)$
- Since this is true for an arbitrary $x\in U$, then universal generalization gives us
  - $\forall x[P(x)\rightarrow \neg Q(x)]$
- This is what we set out to prove.

36

Proofs with Sets

- Given two sets A and B, there are many times when one needs to prove that $A \subseteq B$, or $A=B$.

Proving $A \subseteq B$

- To prove that $A \subseteq B$, one must show that every element in A is also in B.
- To do this, pick an arbitrary element $x \in A$, and show that it is in B.
- Since *x* was chosen arbitrarily, it could just as well have been any element of A, so every element of A is contained in B.

Proving A=B

- One way to show that $A=B$ is to show that $A \subseteq B$ and $B \subseteq A$.

37

Subset Proof

- Let U be the set of integers, $A=\{x \mid x \text{ is even}\}$, $B=\{ x \mid x \text{ is a multiple of } 3\}$, and $C=\{x \mid x \text{ is a multiple of } 6\}$
- Show that $A \cap B=C$.

Proof:

- Let $x \in A \cap B$. Then *x* is a a multiple of 2 and a multiple of 3.
  Therefore *x* is a multiple of 6, and $x \in C$.
  Therefore $A \cap B \subseteq C$.
- Let $x \in C$. Then *x* is a multiple of 6.
  Therefore *x* is a multiple of 2 and a multiple of 3.
  Therefore, $x \in A$ and $x \in B$.
  Since $x \in A$ and $x \in B$, $x \in A \cap B$.
  Therefore, $C \subseteq A \cap B$.
- Since $C \subseteq A \cap B$ and $A \cap B \subseteq C$, $A \cap B=C$.

38

The End

- We hope you have enjoyed this brief introduction to proof techniques.

39