16.070

Introduction to Computers & Programming

Proof Theory 1

Slides based on: Kenneth Rosen's Discrete Mathematics and It's Applications, 5th Edition

Prof. Kristina Lundqvist
Dept. of Aero/Astro, MIT

Methods of Proof

We will introduce some formal rules of reasoning for constructing proofs.

Proof techniques will be introduced formally at first, but as we become more familiar with them, we will gradually start to use these techniques on a more casual and less explicit level. Of course the techniques and proof methods must still be observed in order for your proofs to be valid but you will develop less need to explicitly refer to the steps in order to construct a valid proof.

Definitions

- A **theorem** is a statement that can be shown to be true
- A **proof** is a sequence of statements that forms an argument showing that a theorem is true
- A **fallacy** is an incorrect form of reasoning that is often erroneously believed to be a valid argument. Fallacies are often found in "proofs" of an invalid "theorem"
- A **lemma** is a simple theorem used in the proof of others.
- A **corollary** is a proposition that follows readily from a theorem that has been proved
- A **conjecture** is a statement whose truth value is unknown. When a proof of a conjecture is found, it becomes a theorem

Rules of Inference

We will introduce **rules of inference** for **propositional logic**.

Rules of inference allow you to **take steps in a proof** toward your goal.

A proof starts out with **assumptions** (usually) then by using rules of inference with the assumptions we move closer and closer to the desired result of the theorem.

When we have reached the desired result by ***using only our assumptions and valid rules of inference*** then the **theorem is proved**.

Rule of Inference: Modus Ponens

(p Ù (p ® q)) ® q is a **tautology**. It states that if we know that both an *implication* $p \rightarrow q$ is true and that its *hypothesis*, p, is true, then the *conclusion*, q, is true.

Ex: Suppose the implication "If the bus breaks down, then I will have to walk" and its hypothesis "the bus breaks down" are true. Then by modus ponens it follows that "I will have to walk".

Ex: Assume that the implication $(n > 3) \rightarrow (n^2 > 9)$ is true. [It actually is true, universal quantification]. Suppose also that $n > 3$. Then by modus ponens, it follows that $n^2 > 9$.

Fallacy: Affirming the Conclusion

(q Ù (p ® q)) ® p is a **contingency**. It states that if we know that both an implication $p \rightarrow q$ is true and that its conclusion, q, is true, then the hypothesis, p, is true.

Ex: Suppose the implication "If the bus breaks down, then I will have to walk" and its conclusion "I will have to walk" is true. It **does not** follow that the bus broke down. Perhaps I simply missed the bus.

Ex: Consider the implication $(n > 3) \rightarrow (n^2 > 9)$ which is true. Suppose also that $n^2 > 9$. It does not follow that $n > 3$. It might be that $n = -4$ for example.

Rule of Inference	**Tautology**	**Name**
p $\therefore p \vee q$	$p \rightarrow p \vee q$	Addition
$p \wedge q$ $\therefore p$	$p \wedge q \rightarrow p$	Simplification
p, q $\therefore p \wedge q$	$(p) \wedge (q) \rightarrow p \wedge q$	Conjunction
$p, p \rightarrow q$ $\therefore q$	$p \wedge (p \rightarrow q) \rightarrow q$	Modus Ponens
$\neg q, p \rightarrow q$ $\therefore \neg p$	$\neg q \wedge (p \rightarrow q) \rightarrow \neg p$	Modus Tollens
$p \rightarrow q, q \rightarrow r$ $\therefore p \rightarrow r$	$(p \rightarrow q) \wedge (q \rightarrow r)$ $\rightarrow (p \rightarrow r)$	Hypothetical Syllogism
$p \vee q, \neg p$ $\therefore q$	$(p \vee q) \wedge \neg p \rightarrow q$	Disjunctive Syllogism
$p \vee q, \neg p \vee r$ $\therefore q \vee r$	$(p \vee q) \wedge (\neg p \vee r)$ $\rightarrow q \vee r$	Resolution

Ex: Consider these statements "If I buy something, then I go to the store." and "If I go to the store, then I drive my car." If these two statements are true, then by ***hypothetical syllogism*** we can conclude that "If I buy something, then I drive my car."

Ex: Consider the statements "It is raining today or it is snowing today." and "It is not snowing today or it is windy today." If we know both of these statements are true then **what can we conclude?**

By the ***rule of resolution***, we know that "It is raining today or it is windy today."

Valid Arguments

- An **argument** is called **valid** if whenever all of the *hypotheses* are true then the *conclusion* is true. So to show that q logically follows from p_1, p_2, …, p_n is the same thing as showing that the implication $p_1 \wedge p_2 \wedge \ldots \wedge p_n \rightarrow q$ is a tautology.

Ex: Show that

[(Øp Ù q) Ù **(r ® p)** Ù **(Ør ® s)** Ù **(s ® t)]** ® **t**

is a true statement.

Proof: We assume the hypotheses $(\neg p \wedge q)$, $(r \rightarrow p)$, $(\neg r \rightarrow s)$, and $(s \rightarrow t)$.

1. By $(\neg p \wedge q)$ we know $\neg p$ [simplification].
2. By $(r \rightarrow p)$ we know $\neg p \rightarrow \neg r$ [**contrapositive**].
3. By 2 and $(\neg r \rightarrow s)$ we know $(\neg p \rightarrow s)$ [hypothetical syllogism].
4. By 3 and $(s \rightarrow t)$ we know $(\neg p \rightarrow t)$ [hypothetical syllogism].
5. By 1 and 4 we know **t** [modus ponens].

Resolution

Resolution is a rule of inference that we saw earlier in our table:

$$(p \vee q) \wedge (\neg p \vee r) \rightarrow q \vee r.$$

This rule turns out to be very useful in the field of automated reasoning (trying to get a computer to draw conclusions based on observations). As it turns out the operators Ø, Ú, and Ù form a functionally complete logic system. What this means is that **any statement in proposition that we wish to express, we could express the statement using only these three operators** (though the statement might be substantially longer if we choose to do so). [Transform $\rightarrow$, $\leftrightarrow$, $\oplus$]

Ex: A detective has interviewed four witnesses to a crime. From the stories of the witnesses the detective has concluded that if the butler is telling the truth, then so is the cook; the cook and the gardener can not both be telling the truth; the gardener and the handyman are not both lying; and if the handyman is telling the truth then the cook is lying. For each of the four witnesses, can the detective determine whether that person is telling the truth or lying?

Let us use the first letter of each title to represent the proposition that the person is telling the truth (e.g. h stands for "the handyman is telling the truth). We are given 4 statements which we translate into symbolic propositions using our letters and logical connectives:

(1) $b \rightarrow c$

(2) $\neg(c \wedge g)$ or $\neg c \vee \neg g$

(3) $\neg(\neg g \wedge \neg h)$ or $g \vee h$

(4) $h \rightarrow \neg c$

(1) $b \rightarrow c$

(2) $\neg(c \wedge g)$ or $\neg c \vee \neg g$

(3) $\neg(\neg g \wedge \neg h)$ or $g \vee h$

(4) $h \rightarrow \neg c$

What if the cook were telling the truth? [Use propositions]

By using our propositions and rules of logic, we determine that if the cook is telling the truth then the cook must be lying! So it can not possibly be that the cook is telling the truth. What we have done, basically, is to chain our propositions together to see that this follows:

(5) $c \rightarrow \neg c$ [How can this be? What truth value must c have?]

Now we know that c is false. [What does (1) tell us?]

b is false. Now we know both b and c are false. [(1), (2), (4)?]

They are all satisfied and so give no further info. [What about (3)?]

(3) Says that the gardener is truthful or the handyman or both. [Fal. h...]

(1) $b \rightarrow c$	or	$\neg b \vee c$
(2) $\neg(c \wedge g)$	or	$\neg c \vee \neg g$
(3) $\neg(\neg g \wedge \neg h)$	or	$g \vee h$
(4) $h \rightarrow \neg c$	or	$\neg h \vee \neg c$

By combining (1) and (2) we get (5) $\neg b \vee \neg g$

By combining (1) and (4) we get (6) $\neg b \vee \neg h$

By combining (2) and (3) we get (7) $\neg c \vee h$

By combining (3) and (4) we get (8) $g \vee \neg c$

(1) $\neg b \vee c$

(2) $\neg c \vee \neg g$

(3) $g \vee h$

(4) $\neg h \vee \neg c$

(5) $\neg b \vee \neg g$

(6) $\neg b \vee \neg h$

(7) $\neg c \vee h$

(8) $g \vee \neg c$

By combining (1) and (7) we get (9) $\neg b \vee h$

By combining (1) and (8) we get (10) $\neg b \vee g$

By combining (2) and (8) we get (11) $\neg c \vee \neg c \equiv \neg c$

By combining (3) and (5) we get (9) $\neg b \vee h$

By combining (3) and (6) we get (10) $\neg b \vee g$

By combining (4) and (7) we get (11) $\neg c \vee \neg c \equiv \neg c$

By combining (5) and (8) we get (12) $\neg b \vee \neg c$

By combining (6) and (7) we get (12) $\neg b \vee \neg c$

(1) $\neg b \vee c$	(5) $\neg b \vee \neg g$	(9) $\neg b \vee h$
(2) $\neg c \vee \neg g$	(6) $\neg b \vee \neg h$	(10) $\neg b \vee g$
(3) $g \vee h$	(7) $\neg c \vee h$	(11) $\neg c$
(4) $\neg h \vee \neg c$	(8) $g \vee \neg c$	(12) $\neg b \vee \neg c$

By combining (9) and (4) we get (12) $\neg b \vee \neg c$

By combining (9) and (6) we get (13) $\neg b \vee \neg b \equiv \neg b$

By combining (10) and (2) we get (12) $\neg b \vee \neg c$

By combining (10) and (5) we get (13) $\neg b \vee \neg b \equiv \neg b$

By combining (11) and (1) we get (13) $\neg b$

By combining (12) and (1) we get (13) $\neg b \vee \neg b \equiv \neg b$

We can see that (13) won't combine with anything so we're done.
We have come to the same conclusions as before $\neg b$ and $\neg c$.

Fallacy: Denying the Hypothesis

$(\neg p \wedge (p \rightarrow q)) \rightarrow \neg q$ is a contingency. It states that if we know that both an implication $p \rightarrow q$ is true and that its hypothesis, p, is false, then the conclusion, q, is also false.

Ex: Suppose the implication "If the bus breaks down, then I will have to walk" is true but its hypothesis "the bus breaks down" is false. It does not follow that I will not have to walk. Perhaps I simply missed the bus.

Ex: Consider the implication $(n > 3) \rightarrow (n^2 > 9)$ which is true. Suppose also that $n \leq 3$. It does not follow that $n^2 \leq 9$. It might be that $n = -4$ for example.

Rules of Inference for Quantified Statements

The rules of inference for quantified statements are very important. We use these rules when we construct proofs and they are the basis for proving or disproving a universally or existentially quantified statement.

Universal Instantiation

If we know that " **xP(x)** is true, then we can conclude that **P(c)** is true for a particular member c of the universe of discourse. This is called **universal instantiation** because we are taking an instance, c, from the universe of discourse. This rule is useful when we are given $\forall x P(x)$ as a premise and we know that c is an element of the universe of discourse for x. Then we know P(c) is true.

Ex: We know $\forall x(x^2 \geq 0)$. So by universal instantiation $2^2 \geq 0$.

Universal Generalization

If we know that **P(c)** is true for all elements c in the universe of discourse, then we can conclude that $\forall x P(x)$ is true. This is called **universal generalization**. This rule is often used to prove statements of the form $\forall x P(x)$ by taking an arbitrary element c from the universe of discourse and showing that **P(c)** is true. It is crucial that *c* is an *arbitrary element* from the universe of discourse for this technique to be valid.

Ex: Let c be an integer. We know that c^2 is not negative. So $c^2 \geq 0$. Now by universal generalization (since c was an arbitrary integer) we conclude $\forall x(x^2 \geq 0)$.

Existential Instantiation

If we know that $**xP(x)** is true, then we can conclude that **P(c)** is true for a some member c of the universe of discourse. This is called **existential instantiation** because we are taking an instance, c, from the universe of discourse for which **P(c)** is true. This rule is particularly useful when we are given $**xP(x)** as a premise but we need to discuss a particular element. We can simply give a name, c, for an element of the universe of discourse for which P(c) is true. We may not know anything else about c.

Ex: We know $\exists x(x^2 = 1)$. So by existential instantiation $c^2 = 1$ for some integer c. Now we can talk about c.

Existential Generalization

If we know that **P(c)** is for some particular c in the universe of discourse, then we can conclude that $**xP(x)** is true. This is called **existential generalization**. This rule is often used to prove statements of the form $**xP(x)** by finding a particular c in the universe of discourse such that **P(c)** is true. The alternative to this is to directly show that some element x must exist in the u.d. for which **P(x)** is true without actual finding a particular element.

Ex: $1^2 = 1$. So $\exists x(x^2 = x)$ is true.

Often these four rules are used without explicit reference in a proof. We don't explicitly say, "… by universal generalization …". But we need to be clear enough in our arguments that it is evident what rule we are using. A proof that uses universal generalization to establish $\forall x P(x)$ usually starts off "Let x be an integer". This really means, "Let x be an arbitrary integer". Then we proceed to show that P(x) is true. Once we reach this conclusion, we don't usually go on to state that "since x was an arbitrary integer, then P(x) is established for all integers." We usually just leave it at that once we get to P(x).

By the same token, mathematicians use implicit universal quantification. So the statement "The sum of two odd integers is even" means "for all odd integers x and y, x + y is even". It does not mean that there exists two odd integers whose sum is even.

We will now move on to proof techniques and start putting all of this machinery we have developed to good use.

Methods of Proving Theorems

- We will now discuss approaches to proving theorems. These approaches will use the rules of inference that we have just discussed.

- Many theorems to be proved are implications. So we will concentrate on methods of proving implications.

Direct Proof

To prove the implication, **p ® q**, we must show that whenever the hypothesis (p) is satisfied, then the conclusion (q) must also be true. Remember that an implication is only false in the one case where p is true and q is false. So we must rule out this possibility to show that $p \rightarrow q$ is a tautology.

With a direct approach, we first assume that p is true. Then we use our rules of inference, logical equivalences, and previously proved theorems to show that q must also be true.

Note that it may not be the case that p is true. If p is false then the implication holds. We assume that p is true so that we can explore this scenario and show that q must necessarily be true as well.

Unrelated Definition

Def: The integer n is **even** if there exists an integer k such that $n = 2k$. That is, the integer **n is even if $k(n = 2k)** where the universe of discourse for k is all integers. $[\exists k(n = 2k) \leftrightarrow$ n is even]

Def: The integer n is **odd** if there exists an integer k such that $n = 2k + 1$. That is, the integer **n is odd if $k(n = 2k + 1)** where the universe of discourse for k is all integers. $[\exists k(n = 2k + 1) \leftrightarrow$ n is odd]

Note that an integer is either even or odd (but not both).

[n is even $\leftrightarrow$ n is not odd]

Ex:	7 = 2*3 + 1	[7 is odd]	16 = 2*8	[16 is even]
	-11 = 2*(-6) + 1	[-11 is odd]	-6 = 2*(-3)	[-6 is even]

Ex: Give a direct proof of "**If n is odd, then n^2 is odd**."

First off, recall that this statement is implicitly a universal quantification "$\forall$ **n(n is odd $\rightarrow$ n^2 is odd)**." [What rule do we need?]

Proof: [step 1: Write assumptions]

Let n be an odd integer. [Implicitly arbitrary, set up for U.G.]

[step 2: Translate assumptions into a form we can work with]

Then n = 2k + 1 for some integer k. [Definition of odd]

[step 3: Work with it until it is in a form we need for concl.]

So $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

[step 4: Realize that you're there and state your conclusion.]

So $n^2 = 2*m + 1$ where $m = (2k^2 + 2k)$, so n^2 is odd.♣

$2k^2 + 2k$ is an integer because k is and the integers are closed for +,*,-,^

Proof Simplified

Theorem: If n is odd, then then n^2 is odd.

Proof: Let n be an odd integer. Then n = 2k + 1 for some integer k. So $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. So $n^2 = 2*m + 1$ where $m = (2k^2 + 2k)$, so n^2 is odd.♣

Proof Complicated

Theorem: If n is odd, then then n^2 is odd.

Proof: Assume the hypothesis: let n be an odd integer.

Then n = 2k + 1 for some integer k by the definition of an odd integer.

So by squaring both sides we see that $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

Now by letting $m = 2k^2 + 2k$, we see that $n^2 = 2*m + 1$.

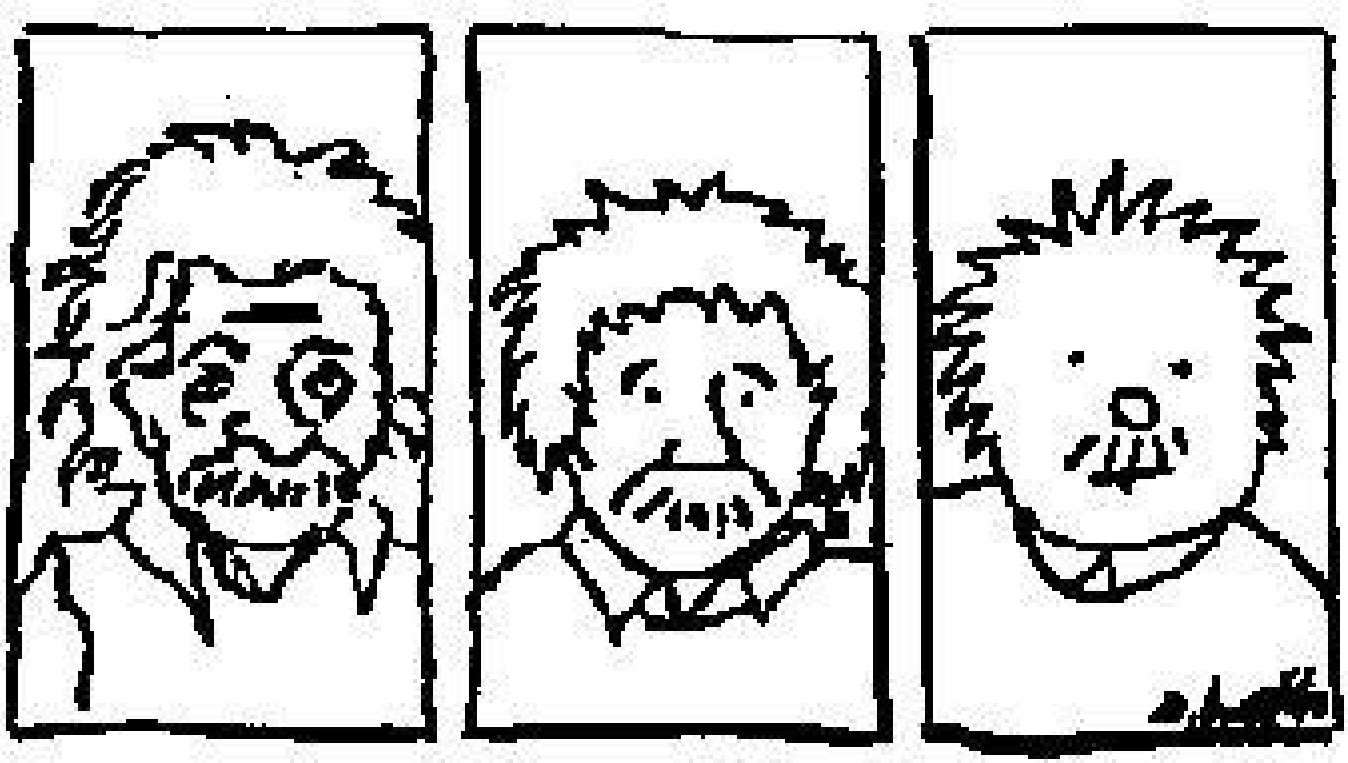
Now m is an integer since 2 and k were integers.

So n^2 is odd by the definition of an odd integer.

Now by universal generalization, since n was chosen as an arbitrary odd integer, then the statement is true for all integers n.♣

"Make everything as simple as possible, but not simpler."
-Albert Einstein

Einstein Simplified



Proof Reversed (meet in the middle)

Theorem: If n is odd, then then n^2 is odd.

Proof: Let n be an odd integer. [Assume the hypothesis as always]

We wish to show that n^2 is odd. [State what we desire to conclude]

To show that n^2 is odd, we must show that $n^2 = 2*m + 1$ for some integer m. [Now we realize that we need to know what n^2 equals]

Well since n is odd then $n = 2k + 1$ for some integer k.

So $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

So $n^2 = 2*m + 1$ where $m = (2k^2 + 2k)$, which is what we wanted to show. So n is odd.♣

Indirect Proof

To prove the implication, $p \rightarrow q$, we can take advantage of the fact that the **contrapositive**, $\neg q \rightarrow \neg p$, is **logically equivalent** to the original statement. We can prove $\neg q \rightarrow \neg p$ via the direct approach and then the original implication, $p \rightarrow q$, is proven.

With an indirect approach, we **first assume that q is false**. Then we use our rules of inference, logical equivalences, and previously proved theorems to show that p must also be false.

Note that it may not be the case that q is false. If q is true then the implication holds. We assume that q is false so that we can explore this scenario and show that p must necessarily be false as well.

Ex: Give an indirect proof of "If 3n + 2 is odd, then n is odd."

Recall again that this statement is implicitly a universal quantification "$\forall n(3n + 2 \text{ is odd} \rightarrow n \text{ is odd})$."

Proof: We will prove the **contrapositive**, "If n is not odd, then 3n + 2 is not odd. That is, "If n is even, then 3n + 2 is even."

[step 1: Write assumptions] Let n be an even integer.

[step 2: Translate assumptions into a form we can work with]

Then n = 2k for some integer k. [Definition of even]

[step 3: Work with it until it is in a form we need for concl.]

So 3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1).

[step 4: Realize that you're there and state your conclusion.]

So 3n + 2 = 2*m where m = (3k + 1), so 3n + 2 is even. ♣

Vacuous and Trivial Proof

To prove the implication, $p \rightarrow q$, we must show that whenever the hypothesis (p) is satisfied, then the conclusion (q) must also be true. Remember that an implication is only false in the one case where p is true and q is false.

If we can show that **p is not ever true** then the **implication is proved**. This is called **vacuous proof**.

Similarly, if we can show that **q is always true** then the **implication is proved**. This is called **trivial proof**.

Ex: Use a **vacuous proof** to show that "If 2n is odd, then 3n is even."

Recall again that this statement is implicitly a universal quantification "$\forall n(2n \text{ is odd} \rightarrow 3n \text{ is even})$."

Proof: Let n be an integer. Then 2n is even by the definition of even. So 2n is not odd. Hence the hypothesis is not satisfied and the implication is shown to be true.♣

Ex: Use a **trivial proof** to show that "If n is odd, then 2n is even."

Recall again that this statement is implicitly a universal quantification "$\forall n(n \text{ is odd} \rightarrow 2n \text{ is even})$."

Proof: Let n be an integer. Then 2n is even by the definition of even. [It doesn't matter if n is odd, which is precisely why this is a trivial proof. I could have started off assuming the hypothesis (n is odd).] Hence the conclusion is satisfied, so the implication is true.♣

Another Unrelated Definition

PseudoDef: A **real number** is some number that can be expressed as $x_1x_2\ldots x_{n.}y_1y_2y_3\ldots$ where the x_i's and y_i's are decimal digits (0,1,2,3,4,5,6,7,8,9) and n is a positive integer. Note that the number of digits to the left of the decimal point must be finite, but the digits to the right of the decimal point extend endlessly.

Ex: Any integer n is also a real number [n.000…]

1/2 is a real number [0.5000…]

Any quotient of integers, n/m is a real number

π is a real number [3.1415926535897…]

$\sqrt{2}$ is a real number [1.414213562373…]

Def: A real number r that can be expressed as a quotient of integers, p/q, with $q \neq 0$ is called **rational**. A real number that is not rational is called **irrational**. [r is rational iff $\exists p \in Z \; \exists q \in Z \; (r = p/q \wedge (q \neq 0))$]

Ex: Any integer n is a rational number [n/1]

1/2 is a rational number [1/2]

π is an irrational number [This is a deep result we will not prove]

$\sqrt{2}$ is an irrational number [We will prove this, but not yet]

Ex: Is 0.75 a rational number?

Yes. It can be expressed as 3/4. [Note that this is not unique, 6/8, etc.]

Ex: Is 5/0.2 a rational number?

Yes. It can be expressed as 25/1. This is a very important point. To know that a number is irrational, it is not enough that the number is expressed as a/b but a or b is not an integer. You must know that there is no way to express it as a quotient of integers.

Ex: Prove that the **sum of two rational numbers is rational**.

Restated: $\forall x \forall y[(x \text{ is rat.}) \wedge (y \text{ is rat.}) \rightarrow \exists z[(z \text{ is rat.}) \wedge (x + y = z)]]$

Proof: [State the assumptions] Let x and y be rational numbers.

[Translate the assumptions into something we can work with.
Remember that we are trying to find out about the sum x + y.]
Since x is rational then x = p/q for some integers p and q where $q \neq 0$.
Since y is rational then y = r/s for some integers r and s where $s \neq 0$.

[Work with it until we get to a form where we need for our concl.]

Then x + y = p/q + r/s = ps/qs + qr/qs = (ps + qr)/qs

[Realize that we have what we need and state the concl. (x + y is rat.)]
(ps + qr) and qs are integers since p,q,r, and s were integers.
$qs \neq 0$ since $q \neq 0$ and $p \neq 0$. [This is something we haven't proved]
So x + y is rational.♣

Which method/technique to use?

We've seen a number of proof techniques so far for proving an implication. Our list of techniques will grow further as we go along. So far we've seen **direct** proof, **indirect** proof, **vacuous** proof, and **trivial** proof.

The question arises, when faced with an implication to prove, "*which method should I use to prove it?*"

As we gain more experience with constructing proofs, you will develop an **intuition** about how to choose. For now, it is mostly a **trial and error process**. You have a number of techniques because often one technique is most suitable to proving a particular theorem.

So if you get stuck, try another technique.

Ex: Prove that **if n is an integer and n^2 is odd, then n is odd**.

Direct Approach: Let **n be an integer such that n^2 is odd**. Then (by the definition of odd), **$n^2 = 2k + 1$ for some integer k**. Now we want to know something about n (namely that *n is odd*). It is difficult to go from *information about n^2 to information about n*. It is much easier to go in the other direction. Let's try an indirect approach.

Indirect Approach: The original statement is $\forall n \in Z$(n^2 is odd $\rightarrow$ n is odd). So the **contrapositive** is $\forall n \in Z$(n is not odd $\rightarrow$ n^2 is not odd). Recalling that a number is not odd iff the number is even, we have: $\forall n \in Z$(n is even $\rightarrow$ n^2 is even).

Let **n be an even integer**. Then (by the definition of even), **$n = 2k$** for some integer k. So **$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$**. Now $2k^2$ is an integer since k is and so we have expressed n^2 as 2(some integer). So by the definition of even, **n^2 is even**.♣

Proof by Contradiction

We have already worked with the concept of proof by **contradiction** on an informal basis. The essence of proof by contradiction is:

Let's say that we want to **prove** some **proposition r**. We may have initial assumptions that we have made and can use to prove this. An approach that we may try is to **assume that r does not hold**. That is, assume Ø**r**. Then if we can use our original assumptions, along with what ¬r tells us, to **come to a logical contradiction** then we know that Ø**r can not possibly be the case**. **So r must be true**.

This is a very detailed and strict proof technique. You must be *extremely careful* when applying this technique that you follow the rules. Misapplication of this technique leads to all sorts of invalid reasoning.

Let's consider the specific case where the statement r that you are trying to prove is an implication of the form $p \rightarrow q$.

If we apply **proof by contradiction** to such a statement, we want to prove r (which is $p \rightarrow q$). So we assume Ø**r**, and then show that this assumption leads to a contradiction. Hence we will have shown that ¬r can't possibly be the case, so we can conclude that r must be true.

What is ¬r?

$\neg r = \neg(p \rightarrow q) \equiv \neg(\neg p \vee q) \equiv \neg\neg p \wedge \neg q \equiv p \wedge \neg q$.

So to assume Ø**r**, we assume **p** Ù Ø**q** (this is exactly the only case when the implication $p \rightarrow q$ is false, when p is true and q is false). Then we show that this assumption leads to a contradiction, and hence we can't ever encounter this situation, so the implication must be true.

In summary, if we wish to **prove an implication p ® q** using the technique of proof by contradiction then we: **Assume p. Assume Øq. Derive a contradiction from these assumptions**.

Ex: Give proof by contradiction that "If 3n + 2 is odd, then n is odd."

Proof: [As *always*, we begin by writing our **assumptions**]. Let n be an integer such that 3n + 2 is odd.

Now we wish to **show** that **n is odd**. So let us assume to the contrary that n is not odd. That is, we are **assuming that n is even**.

Since n is even, then **n = 2k** for some integer k.

So 3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1).

So 3n + 2 = 2*m where m = (3k + 1), so **3n + 2 is even**.

But our original assumption was that **3n + 2 is odd**. We know that an integer is either even or odd but not both, so this is a **contradiction**. 3n + 2 can not be both odd and even. So our assumption (to the contrary) that n was even, must have been in error. **So n must be odd.**♣

Observations about the proof

We **assumed two things** in the proof. We first assumed our hypothesis that "**n is an integer such that 3n + 2 is odd**", then we further assumed that "**n is not odd**". At the end (after we had reached a contradiction based on these two assumptions) we concluded that the assumption that "n is not odd" was in error. Why is it necessarily this assumption that was in error? Could it have been the assumption "n is an integer such that 3n + 2 is odd"?

Of course it could have been either assumption that was in error! All we know is that by assuming both things, we come to a contradiction. So what we have shown is that both things can't be true at once. But remember that we wanted to show "If 3n + 2 is odd, then n is odd." So assuming that 3n + 2 is odd, we concluded that it can't also be true that n is **not** odd. So if 3n + 2 is odd, then n must be odd. This is what we wanted to show.

So remember that with a proof by contradiction you make some assumptions. When you reach a contradiction based on these assumptions then you know that at least one of the assumptions you made can't be. That is, not all of your assumptions can be true at the same time.

So if you are trying to prove $p \rightarrow q$, then you would first assume p. If you were going to use a direct approach, then you would proceed to use the assumption p to show that q necessarily follows. But a proof by contradiction would instead (after assuming p) now assume $\neg q$. Then you would proceed to find a contradiction from these two assumptions. So you would know that p and $\neg q$ can't both be true at the same time. Or equivalently, if p is true, then $\neg q$ can't be true. That is, if p is true then q must be true as well.

Exam

- Everything since last exam until today's lecture
  - B11.1-11.5
  - B4.5
  - F14
  - Handouts