CSI 2101 / Rules of Inference (§1.5)

- **Introduction**
  - what is a proof?
- **Valid arguments in Propositional Logic**
  - equivalence of quantified expressions
- **Rules of Inference in Propositional Logic**
  - the rules
  - using rules of inference to build arguments
  - common fallacies
- **Rules of Inference for Quantified Statements**

Proof?

- In mathematics, a *proof* is a *correct (well-reasoned, logically valid) and complete (clear, detailed) argument that rigorously & undeniably establishes the truth of a mathematical statement.*
- Why must the argument be correct & complete?
  - *Correctness* prevents us from fooling ourselves.
  - *Completeness* allows anyone to verify the result.

Proof?

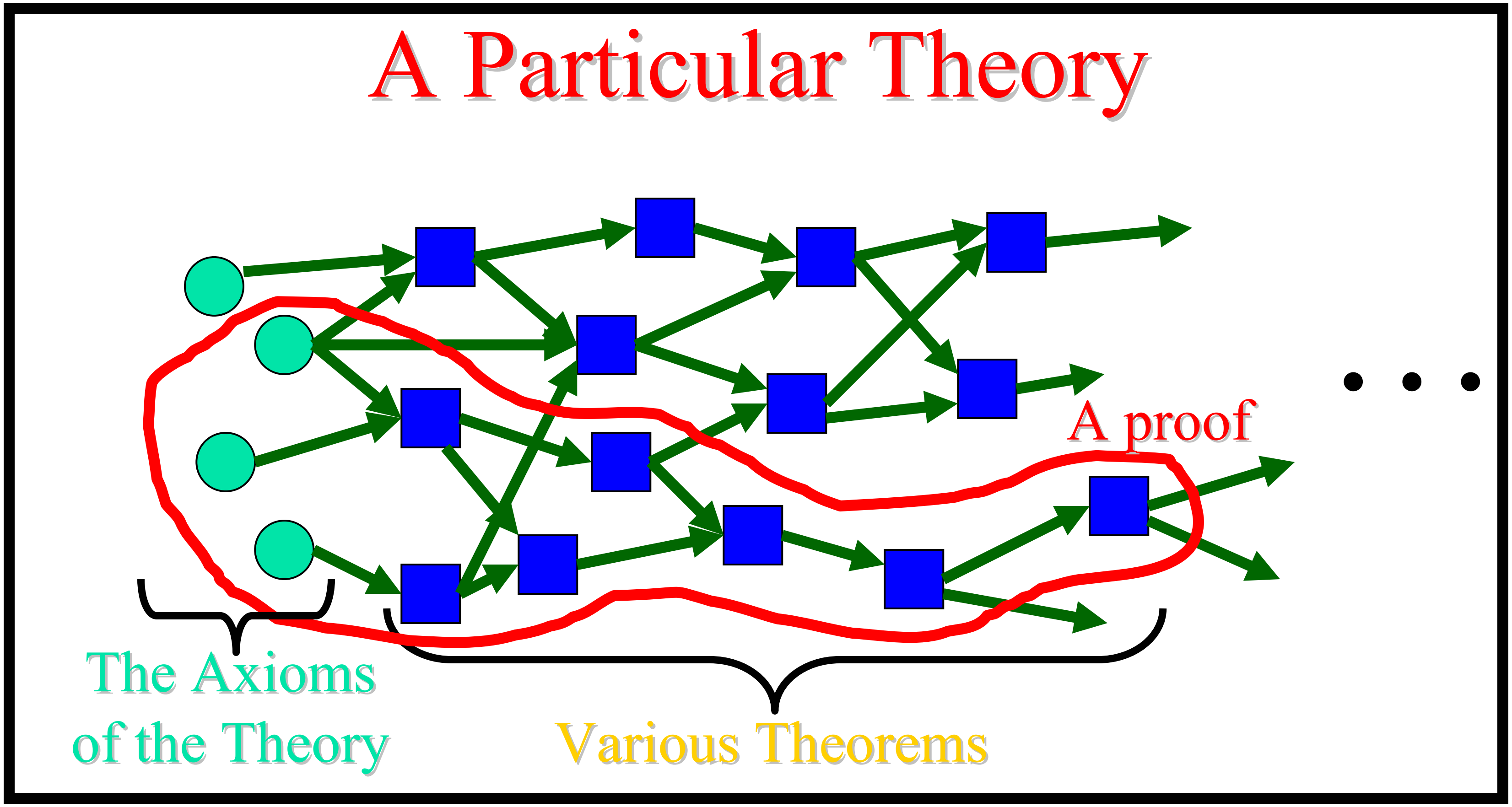
Applications of Proofs

- An exercise in clear communication of logical arguments in any area of study.
- The fundamental activity of mathematics is the discovery and elucidation, through proofs, of interesting new theorems.
- Theorem-proving has applications in program verification, computer security, automated reasoning systems, *etc.*
- Proving a theorem allows us to rely upon on its correctness even in the most critical scenarios.

Terminology

- *Theorem*: A statement that has been proven to be true.
- *Axioms, postulates, hypotheses, premises*: Assumptions (often unproven) defining the structures about which we are reasoning.
- *Rules of inference*: Patterns of logically valid deductions from hypotheses to conclusions.
- *Lemma:* A minor theorem used as a stepping-stone to proving a major theorem.
- *Corollary:* A minor theorem proved as an easy consequence of a major theorem.
- *Conjecture:* A statement whose truth value has not been proven. (A conjecture may be widely believed to be true, regardless.)
- *Theory:* The set of all theorems that can be proven from a given set of axioms.

Graphical Visualization



How to prove something?

Consider the statements:

- If you did not sleep last night, you will sleep during the lecture.
- You did not sleep last night

We can conclude that you will sleep during the lecture.

Let P be "you did not sleep last night"

and Q be "you will sleep during the lecture"

The **form** of our argument is:

P → Q
P

Q

which reflects tautology:

$$((p \to q) \wedge p) \to q$$

Rules of Inference

Any valid argument form can be used

- there are infinitely many of them, based on different tautologies
- validity of an argument form can be verified e.g. using truth tables

There are simple, commonly used and useful argument forms

- when writing proofs for humans, it is good to use well known argument forms
  - so that the reader can follow
  - complex argument forms can be derived from simpler ones

Although the original idea was to have a mechanical approach to proofs

Rules of Inference

- An *Inference Rule* is
  - A pattern establishing that if we know that a set of *antecedent* statements of certain forms are all true, then we can validly deduce that a certain related *consequent* statement is true.
- $$\begin{array}{l} \textit{antecedent 1} \\ \textit{antecedent 2 \ldots} \\ \hline \therefore\ \textit{consequent} \end{array}$$

"∴" means "therefore"

Each valid logical inference rule corresponds to an implication that is a tautology.

Corresponding tautology: $((\textit{ante. 1}) \land (\textit{ante. 2}) \land \ldots) \rightarrow \textit{consequent}$

Some Inference Rules

- $$\frac{p}{\therefore\ p \vee q}$$ Rule of Addition
- $$\frac{p \wedge q}{\therefore\ p}$$ Rule of Simplification
- $$\begin{array}{l} p \\ q \\ \hline \therefore\ p \wedge q \end{array}$$ Rule of Conjunction

Modus Ponens & Tollens

- $$\left.\begin{array}{r} p \\ \underline{p \to q} \\ \therefore q \end{array}\right\}$$

  Rule of *modus ponens* (a.k.a. *law of detachment*)

  “the mode of affirming”

- $$\left.\begin{array}{r} \neg q \\ \underline{p \to q} \\ \therefore \neg p \end{array}\right\}$$

  “the mode of denying”

  Rule of *modus tollens*

Syllogism & Resolution Inference Rules

$$\begin{array}{l} p \to q \\ \underline{\quad q \to r} \\ \therefore p \to r \end{array}$$

Rule of hypothetical syllogism

$$\begin{array}{l} p \vee q \\ \underline{\quad \neg p \quad} \\ \therefore\ q \end{array}$$

Rule of disjunctive syllogism

$$\begin{array}{l} \quad p \vee q \\ \underline{\neg p \vee r} \\ \therefore q \vee r \end{array}$$

Rule of Resolution

Formal Proofs

- A formal proof of a conclusion *C*, given premises $p_1, p_2,\ldots,p_n$ consists of a sequence of *steps*, each of which applies some inference rule to premises or previously-proven statements (*antecedents*) to yield a new true statement (the *consequent*).
- A proof demonstrates that *if* the premises are true, *then* the conclusion is true.

Formal Proof Example

- Suppose we have the following premises:
“It is not sunny and it is cold.”
“We will swim only if it is sunny.”
“If we do not swim, then we will canoe.”
“If we canoe, then we will be home early.”
- Given these premises, prove the theorem **“We will be home early”** using inference rules.

Proof Example *cont.*

Let us adopt the following abbreviations:

- *sunny* = **“It is sunny”**;
- *cold* = **“It is cold”**;
  swim = **“We will swim”**;
- *canoe* = **“We will canoe”**;
- *early* = **“We will be home early”**.

- Then, the premises can be written as:
  (1) $\neg sunny \wedge cold$ (2) $swim \rightarrow sunny$
  (3) $\neg swim \rightarrow canoe$ (4) $canoe \rightarrow early$

Proof Example *cont.*

Step	Proved by
1. $\neg \mathit{sunny} \land \mathit{cold}$	Premise #1.
2. $\neg \mathit{sunny}$	Simplification of 1.
3. $\mathit{swim} \to \mathit{sunny}$	Premise #2.
4. $\neg \mathit{swim}$	Modus tollens on 2,3.
5. $\neg \mathit{swim} \to \mathit{canoe}$	Premise #3.
6. canoe	Modus ponens on 4,5.
7. $\mathit{canoe} \to \mathit{early}$	Premise #4.
8. early	Modus ponens on 6,7.

Exercises

Which rules of inference are used in:

- It is snowing or it is raining. It is not snowing, therefore it is raining.
- If there is snow I will go snowboarding. If I go snowboarding, I will skip the class. There is snow, therefore I will skip the class.
- I am rich or I have to work. I am not rich or I like playing hockey. Therefore I have to work or I like playing hockey .
- I you are blonde then you are smart. You are smart therefore you are blonde.

$$\begin{array}{l} S \vee \mathrm{R} \\ \neg S \\ \hline \therefore\ \mathrm{R} \end{array}$$

$$\begin{array}{l} S \to B \\ \mathrm{B} \to \mathrm{K} \\ S \\ \hline \therefore \mathrm{K} \end{array}$$

$$\begin{array}{l} \mathrm{R} \vee \mathrm{W} \\ \neg R \vee H \\ \hline \mathrm{W} \vee \mathrm{H} \end{array}$$

WRONG

$$\begin{array}{l} B \to S \\ S \\ \hline \therefore \mathrm{B} \end{array}$$

Using rules of inference to build arguments

Show that: “If it does not rain or if is not foggy, then the sailing race will be held and the lifesaving demonstration will go on. If the sailing race is held, then the trophy will be awarded. The trophy was not awarded.” implies “It rained”

#	Proposition	Rule
1	$(\neg R \vee \neg F) \rightarrow (S \wedge L)$	hypothesis
2	$S \rightarrow T$	hypothesis
3	$\neg T$	hypothesis
4	$\neg S$	modus tollens 2 & 3
5	$\neg S \vee \neg L$	addition to 4
6	$R \wedge F$	modus tollens 1 & 5
7	R	simplification of 6

Examples

What can be concluded from:

- "I am either clever or lucky. I am not lucky. If I am lucky I will win the lottery."

$C \vee L$
$\neg L$
$\underline{L \to T}$
$\therefore$???

- "All rodents gnaw their food. Mice are rodents. Rabbits do not gnaw their food. Bats are not rodents."

R "rodent"
G "Gnaw their food"
B "Rabit"
M "Mousse"
T "Bat"

$R \to G$
$M \to R$
$B \to \neg G$
$\underline{T \to \neg R}$
$\therefore$???

Resolution

The rule

$$
\begin{array}{l}
p \vee q \\
\neg p \vee r \\
\text{-------} \\
\therefore\ q \vee r
\end{array}
$$

is called resolution and is used in computer (automatic) theorem proving/reasoning

- also basis of logical programming languages like Prolog

If all hypotheses and the conclusion are expressed as **clauses** (disjunction of variables or their negations), we can use resolution as the only rule of inference.

Resolution

Express as a (list of) clause(s):

- $p \vee (q \wedge r)$ $(p \vee q) \wedge (p \vee r)$
- $\neg(p \vee q)$ $(\neg p) \wedge (q)$
- $p \rightarrow q$ $(\neg p \vee q)$
- $\neg(p \leftrightarrow q)$

$$\neg((\neg p \vee q) \wedge (\neg q \vee p))$$
$$= \neg(\neg p \vee q) \vee \neg(\neg q \vee p)$$
$$= (p \wedge \neg q) \vee (\neg\, p \wedge q)$$
$$= ((p \wedge \neg q) \vee (\neg\, p)) \wedge ((p \wedge \neg q) \vee q))$$
$$= (\neg q \vee \neg\, p) \wedge (p \vee q)$$

Use the rule of resolution to show that

$(p \vee q) \wedge (\neg p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee \neg q)$ is not certifiable

$(q \wedge \neg q) = \mathbf{F}$

Rules of Inference for Quantified Statements

$\dfrac{(\forall x)\ P(x)}{\therefore P(c)}$	Universal Instantiation
$\dfrac{P(c) \text{ for an arbitrary } c}{\therefore (\forall x)\ P(x)}$	Universal Generalization
$\dfrac{\exists(x)\ P(x)}{\therefore\ P(c) \text{ for some element } c}$	Existential Instantiation
$\dfrac{P(c) \text{ for some element } c}{\therefore\ \exists(x)\ P(x)}$	Existential Generalization

Review

Commonly used argument forms of propositional logic

- modus ponens, modus tollens, hypothetical syllogism (transitivity of implication), disjunctive syllogism, addition, simplification, conjunction, resolution

Rules of inference for quantified statements

- universal instantiation, universal generalization
- existential instantiation, existential generalization

Resolution and logical programming

- have everything expressed as clauses
- it is enough to use only resolution

Combining Rules of Inference

$\forall x\,(P(x) \to Q(x))$
$P(a)$

$\therefore\ Q(a)$

Universal modus ponens

$\forall x\,(P(x) \to Q(x))$
$\neg Q(a)$

$\therefore\ \neg P(a)$

Universal modus tollens

#	Statement	Rule
1	$\forall x\,(P(x) \to Q(x))$	hypothesis
2	$P(a)$	hypothesis
3	$P(a) \to Q(a)$	universal instantiation
4	$Q(a)$	modus ponens 2 & 3

Examples/exercises

Use rules of inference to show that if

$\forall x\ (P(x) \lor Q(x))$

$\forall x(\neg Q(x) \lor S(x))$

$\forall x\ (R(x) \rightarrow \neg S(x)$ and

$\exists x\ \neg P(x)$ are true, then also

$\exists x\ \neg R(x)$ is true

$\forall x\ (P(x) \lor Q(x))$ and $\forall x(\neg Q(x) \lor S(x))$ implies $\forall x(P(x) \lor S(x))$

$\forall x\ (R(x) \rightarrow \neg S(x)$ is equivalent to $\forall x(\neg\ S(x) \lor \neg\ R(x))$

Therefore $\forall x(P(x) \lor \neg R(x))$

Since $\exists x\ \neg P(x)$ is true. Thus $\neg P(a)$ for some a in the domain. Since $P(a) \lor \neg R(a)$ must be true.

Conclusion $\neg R(a)$ is true and so $\exists x\ \neg R(x)$ is true

Examples/exercises

What is wrong in this argument, “proving” that

- $\exists x P(x) \wedge \exists x Q(x)$ implies $\exists x (P(x) \wedge Q(x))$

1.	$\exists x P(x) \wedge \exists x Q(x)$		premise
2.	$\exists x P(x)$		simplification from 1.
3.	$P(c)$		universal instantiation from 2.
4.	$\exists x Q(x)$		simplification from 1.
5.	$Q(c)$	c????	universal instantiation from 4
6.	$P(c) \wedge Q(c)$		conjunction from 3. and 5.
7.	$\exists x (P(x) \wedge Q(x))$		existential generalization

Examples/exercises

- Is the following argument valid?

  If Superman were able and willing to prevent evil, he would do so.

  Is Superman were unable to prevent evil, he would be impotent; if he were unwilling to prevent evil, he would be malevolent.

  Superman does not prevent evil.

  If Superman exists, he is neither impotent nor malevolent.

  Therefore, Superman does not exist.

$$\begin{array}{l}
A \wedge W \to P \\
\neg A \to I \\
\neg W \to M \\
\neg P \\
E \to \neg I \wedge \neg M \\
\hline
\neg E
\end{array}$$

From $A \wedge W \to P$ and $\neg P$ we deduce $\neg(A \wedge W)$.

$\neg A \vee \neg W$ (1)

$\neg A \to I$ thus $A \vee I$ (2)

$\neg W \to M$ thus $W \vee M$ (3)

(4)=(1)&(2) $I \vee \neg W$

(1) & (4) $\neg A \vee I$,,,,,,,,

OK so what is a proof?

Formal proof

- sequence of statements, ending in conclusion
- statements preceding the conclusion are called premises
- each statement is either an axiom, or is derived from previous premises using a rule of inference

Informal proof

- formal proofs are too tedious to read
- humans don't need that much detail, obvious/easy steps are skipped/grouped together
- some axioms may be skipped (implicitly assumed)
- we will now talk about how to write informal proofs
  - which are still formal and precise enough

Terminology

- *Theorem*: A statement that has been proven to be true.
- *Axioms, postulates, hypotheses, premises*: Assumptions (often unproven) defining the structures about which we are reasoning.
- *Rules of inference*: Patterns of logically valid deductions from hypotheses to conclusions.
- *Lemma:* A minor theorem used as a stepping-stone to proving a major theorem.
- *Corollary:* A minor theorem proved as an easy consequence of a major theorem.
- *Conjecture:* A statement whose truth value has not been proven. (A conjecture may be widely believed to be true, regardless.)
- *Theory:* The set of all theorems that can be proven from a given set of axioms.

OK so how to prove a theorem?

Depends on how the theorem looks like

- A simple case – **proving existential statements** ∃ x P(x):

There is an even integer that can be written in two ways as a sum of two prime numbers

How to prove this proposition?

- find such x and the four prime numbers “10 = 5+5 = 3+7” DONE

For every integer x there is another integer y such that y > x. ∀x ∃ y: y>x

- Enough to show how to find such y for every integer x:
  - just take y = x+1

Both are **constructive proofs** of existence

There exist also non-constructive proofs

- but constructive are more useful

Proving by Counterexample

Another simple case

disproving the negation of existential statements: $\neg\exists$ **x P(x)**

disproving universal statements

- by giving an counterexample

Examples:

Disprove: For all real numbers a and b, if $a^2 = b^2$ then $a = b$

Disprove: There are no integers x such that $x^2 = x$.

These are constructive proofs

- yes, you can also have non-constructive ones

How to disprove an existential theorem?

By proving the negation, which is a universal statement.

Example: Disprove: There is a positive integer such that n^2+3n+2 is prime

We are going to prove: For every positive integer n, n^2+3n+2 is not prime.

Proof:

Suppose n is any positive integer. We can factor n^2+3n+2 to obtain $n^2+3n+2 = (n+1)(n+2)$.

Since $n \geq 1$ therefore $n+1>1$ and $n+2>1$. Both n+1 and n+2 are integers, because they are sums of integers.

As n^2+3n+2 is a product of two integers larger than 1, it cannot be prime.

How to prove a universal theorem?

Most theorems are universal of the form $\forall x\ P(x) \rightarrow Q(x)$

by exhaustion

- if the domain is finite
- or the number of x for which P(x) holds is finite

Example: $\forall x$ x is even integer such that $4 \leq x \leq 16$, x can be written as a sum of two prime numbers

- 4=2+2, 6=3+3, 8=3+5, 10=5+5, 12 = 5+7, 14 = 7+7, 16 = 3+13

Exhaustion does not work when the domain is infinite, or even very large

- you don't want to prove that the multiplication circuit in the CPU is correct for every input by going over all possible inputs

How to prove a universal theorem?

Most theorems are universal of the form $\forall x\, P(x) \rightarrow Q(x)$

How to prove that?

- **generalizing from the generic particular**
- Let x be a particular, but arbitrarily chosen element from the domain, show that if x satisfies P then it also must satisfy Q
  - the showing is done as discussed in the last lecture
  - using definitions, previously established results and rules of inference
  - it is important to use only properties that apply to all elements of the domain

This way (assume P(x) and derive Q(x) of proving a statement is called a **direct** proof

Example 1: Direct Proof

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

Definition: The integer is even if there exists an integer k such that n = 2k, and n is odd if there exists an integer k such that n = 2k+1. An integer is even or odd; and no integer is both even and odd.

Theorem: $\forall(n)\ P(n) \rightarrow Q(n)$,

where P(n) is "n is an odd integer" and Q(n) is "n^2 is odd."

We will show $P(n) \rightarrow Q(n)$

Example 1: Direct Proof

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

Proof:

Let p --- "n is odd integer"; q --- "n^2 is odd";
we want to show that p → q.

Assume p, i.e., n is odd. By definition n = 2k + 1, where k is some integer.

Therefore $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$
$= 2(2k^2 + 2k) + 1$, which is by definition an odd number ($k' = (2k^2 + 2k)$).

QED

Example 2: Direct Proof

Theorem: The sum of two even integers is even.

- Starting point: let m and n be arbitrary even integers
- To show: n+m is even

Proof:

Let m and n be arbitrary even integers. Then, by definition of even, m=2r and n=2s for some integers r and s. Then

m+n = 2r+2s (by substitution)

= 2(r+s) (by factoring out 2)

Let k = r+s. Since r and s are integers, therefore also k is an integer. Hence, m+n = 2k, where k is an integer. If follows by definition of even that m+n is even.

Directions for writing proofs

- **be clean and complete**
- **state the theorem to be proven**
- **clearly mark the beginning of the proof (i.e. Proof:)**
- **make the proof self-contained:** introduce/identify all variables
  - "Let m and n be arbitrary even numbers"
  - "… for some integers r and s"
- **write in full sentences** **"**Then m+n = 2r+2s = 2(r+s)."
- **give a reason for each assertion**
  - by hypothesis, by definition of even, by substitution
- **use the connecting little words** to make the logic of the argument clear
  - The, Thus, Hence, Therefore, Observe that, Note that, Let

Examples/exercises

Theorem: The square of an even number is divisible by 4.

Theorem: The product of any three consecutive integers is divisible by 6.

Very Basics of Number Theory

Definition: An integer n is ***even*** iff $\exists$ integer k such that $n = 2k$

Definition: An integer n is ***odd*** iff $\exists$ integer k such that $n = 2k+1$

Definition: Let k and n be integers. We say that k ***divides*** n (and write $k \mid n$) if and only if there exists an integer a such that $n = ka$.

Definition: An integer n is ***prime*** if and only if $n>1$ and for all positive integers r and s, if $n = rs$, then $r=1$ or $s = 1$.

Definition: A real number r is ***rational*** if and only if $\exists$ integers a and b such that $r= a/b$ and $b \neq 0$.

So, which of these numbers are rational?

- 7/13 0.3 3.142857
- 3.142857142857142857142857142857…
- 3/4+5/7

Examples/exercises

Theorem: The square of an even number is divisible by 4.

Proof:

Let n be arbitrary even integer. Then, by definition of even, m=2r for some integers r. Then n2 = (2r)2= 4r2. Therefore and by definition n2 is divisible by 4.

Examples/exercises

Theorem: The product of any three consecutive integers is divisible by 6.

I knew how to prove this, because I had some knowledge of **number theory.**

Definition: Let **k** and **n** be integers. We say that **k** ***divides*** **n** (and write **k | n**) if and only if there exists an integer **a** such that **n = ka**.

Lemma 1: $\forall$ integers **k,n,a: k | n** $\rightarrow$ **k | an**

Lemma2: Out of **k** consecutive integers, exactly one is divisible by **k**.

Lemma 3: $\forall$**x:** $2| x \wedge 3| x \rightarrow 6| x$

(a special case of a more general theorem) $\forall$ x, y, z: $y | x \wedge z|x \rightarrow yz/GCD(y,z) | x$

(will prove Proposition 2 and Lemma 3 afterward, when we know more about number theory)

Proof of Theorem

Theorem: The product of any three consecutive integers is divisible by 6.

Proof: Let n be an arbitrary integer.

From Lemma 2 it follows that either $2|n$ or $2|(n+1)$. Combining with Lemma 1 we deduce that $2|n(n+1)$ and therefore (applying Lemma 1 once more) also $2|n(n+1)(n+2)$.

By Lemma 2 it follows that $3|n$ or $3|(n+1)$ or $3|(n+2)$. Applying Lemma 1 twice we obtain $3|n(n+1)(n+2)$.

Therefore $2 \mid n(n+1)(n+2)$ and $3 \mid n(n+1)(n+1)$. According to Lemma 1 it follows that $6=2*3 \mid n(n+1)(n+2)$

Proof by Contradiction

A – We want to prove p.

We show that:

(1) $\neg p \rightarrow F$; (i.e., a False statement)

(2) We conclude that $\neg p$ is false since (1) is True and therefore p is True.

B – We want to show $p \rightarrow q$

(1) Assume the negation of the conclusion, i.e., $\neg q$

(2) Use show that $(p \wedge \neg q) \rightarrow F$

(3) Since $((p \wedge \neg q) \rightarrow F) \Leftrightarrow (p \rightarrow q)$ (why?) we are done

Example 1: Proof by Contradiction

Theorem “If 3n+2 is odd, then n is odd”

Let p = “3n+2 is odd” and q = “n is odd”

1 – assume p and $\neg q$ i.e., 3n+2 is odd and n is not odd

2 – because n is not odd, it is even

3 – if n is even, n = 2k for some k, and therefore 3n+2 = 3 (2k) + 2 = 2 (3k + 1), which is even

4 so we have a contradiction, 3n+2 is odd and 3n+2 is even therefore we conclude $p \rightarrow q$, i.e., “If 3n+2 is odd, then n is odd”

Q.E.D.

Example2: Proof by Contradiction

Classic proof that √2 is irrational.

- Suppose √2 is rational. Then √2 = a/b for some integers a and b (relatively prime).
- Thus $2 = a^2/b^2$ and then $2b^2 = a^2$.
- Therefore a^2 is even and so a is even, that is (a=2k for some k).
- We deduce that $2b^2 = (2k)^2 = 4k^2$ and so $b^2 = 2k^2$
- Therefore b^2 is even, and so b is even (b = 2k for some k

But if a and b are both even, then they are not relatively prime!

contradiction

Example2: Proof by Contradiction

You're going to let me get away with that?

- a^2 is even, and so a is even (a = 2k for some k)??
- Suppose to the contrary that a is not even.
  - Then a = 2k + 1 for some integer k
  - Then $a^2 = (2k + 1)(2k + 1) = 4k2 + 4k + 1$
  - Therefore a^2 is odd.

contradiction

- So a really is even.

More examples/exercises

Examples:

- there is no greatest integer
- **Proposition 2:** Out of **k** consecutive integers, exactly one is divisible by **k**.
- there is no greatest prime number

OK, we know what is an irrational number, and we know there is one $\sqrt{2}$

- the sum of an irrational number and an rational number is irrational
- there exist irrational numbers **a** and **b** such that a^b is rational
  - non-constructive existential proof

Proof by contraposition

Proof by contraposition

- we want to prove $\forall x\ (P(x) \rightarrow Q(x))$
- rewrite as $\forall x\ (\neg Q(x) \rightarrow \neg P(x))$ (contrapositive of the original)
- prove the contrapositive using direct proof:
  - let x is an arbitrary element of the domain such that Q(x) is false
  - show that P(x) is true

Example 1: Proof by Contraposition

Proof of a statement $p \to q$

Use the equivalence to : $\neg q \to \neg p$ (the contrapositive)

So, we can prove the implication $p \to q$ by first assuming $\neg q$, and showing that $\neg p$ follows.

Example: Prove that if a and b are integers, and $a + b \geq 15$, then $a \geq 8$ or $b \geq 8$.

$$(a + b \geq 15) \to (a \geq 8) \vee (b \geq 8)$$

(Assume $\neg q$)
(Show $\neg p$)

Suppose $(a < 8) \wedge (b < 8)$.
Then $(a \leq 7) \wedge (b \leq 7)$.
Therefore $(a + b) \leq 14$.
Thus $(a + b) < 15$.

QED

Example 2: Proof by Contraposition

Theorem:

For n integer , if 3n + 2 is odd, then n is odd.

I.e. For n integer, 3n+2 is odd $\rightarrow$ n is odd

Proof by Contraposition:

Let p --- "3n + 2" is odd; q --- "n is odd"; we want to show that $p \rightarrow q$

The contraposition of our theorem is $\neg q \rightarrow \neg p$

n is even → 3n + 2 is even

Now we can use a direct proof:

Assume $\neg q$, i.e, n is even therefore n = 2 k for some k.

Therefore $3 n + 2 = 3 (2k) + 2 = 6 k + 2 = 2 (3k + 1)$ which is even.

QED

Contradiction vs Contraposition

Can we convert every proof by contraposition into proof by contradiction?

Proof of $\forall x\, (P(x) \rightarrow Q(x))$ by contraposition:

Let c is an arbitrary element such that Q(c) is false

… (sequence of steps)

$\neg P(c)$

Proof of $\forall x\, (P(x) \rightarrow Q(x))$ by contradiction:

Let $\exists x$ such that P(x) and $\neg Q(x)$

then $\neg Q(c)$ // existential instantiation

… same sequence of steps

Contradiction: P(c) and $\neg P(c)$

Contradiction vs Contraposition

So, which one to use?

Contraposition advantage:

- you don't have to make potentially error-prone negation of the statement
- you know what you want to prove

Contraposition disadvantage:

- usable only for statements that are universal and conditional

Proof Strategy

Statement: For all elements in the domain, if P(x) then Q(x)

Imagine elements which satisfy P(x). Ask yourself “Must they satisfy Q(x)?”

- if you feel “yes”, use the reasons why you feel so as a basis of direct proof
- if it is not clear that “yes” is the answer, think why you think so, maybe that will guide you to find a counterexample
- if you can’t find a counterexample, try to think/observe why
  - maybe from assuming that $P(x) \wedge \neg Q(x)$ you can derive contradiction
  - maybe from assuming that $P(x) \wedge \neg Q(x)$ you can derive $\neg P(x)$

There are no easy ‘cookbooks’ for proofs

- but seeing many different proofs (and yourself proving statements) you learn many useful techniques and tricks that might be applicable

More examples/exercises

Prove that there are no integer solutions for $x^2+3y^2=8$

Prove that there are no integer solutions for $x^2-y^2 = 14$

Prove there is a winning strategy for the first player in the Chomp game

Prove that a chessboard can be tiled by dominoes.

Prove that a chessboard without a corner cannot be tiled by dominoes.

Prove that a chessboard with diagonal corners removed cannot be tiled by dominoes.

More examples/exercises

Prove that $x^n+y^n = z^n$ has no integers solutions with $xyz \neq 0$ for $n>2$.

Fermat's last theorem (took hundreds of years to prove, the proof is hundreds of pages)

The 3x+1 conjecture: Does this program terminate for every integer i?

```
while(i>1) {
    if (even(x)) x = x/2;
    else x = 3x+1;
}
```

Common Mistakes

- **arguing from examples**
  - we notice that 3, 5, 7, 11, 13, 17, 19 are prime, we therefore conclude that all odd numbers are prime???
  - the code produces correct output for the test cases, therefore it will always produce correct output
- **using the same letter to mean two different things**
  - $\exists x P(x) \wedge \exists x Q(x)$ does not imply there is c such that $(P(c) \wedge Q(c))$

Common Mistakes

Some other common mistakes:

1. The mistake of Affirming the Consequent
2. The mistake of Denying the Antecedent
3. Begging the question or circular reasoning

The Mistake of Affirming the Consequent

If the butler did it he has blood on his hands.
The butler had blood on his hands.
Therefore, the butler did it.

This argument has the form

$$\begin{array}{l} P \to Q \\ Q \\ \hline \therefore\ P \end{array}$$

or $((P \to Q) \wedge Q) \to P$ which is not a tautology and therefore not a valid rule of inference

The Mistake of Denying the Antecedent

If the butler is nervous, he did it.

The butler is really mellow.

Therefore, the butler didn't do it.

This argument has the form

$$\begin{array}{l} P \rightarrow Q \\ \neg P \\ \hline \therefore \neg Q \end{array}$$

or $((P \rightarrow Q) \wedge \neg P) \rightarrow \neg Q$ which is not a tautology and therefore not a valid rule of inference

Begging the question or circular reasoning

- This occurs when we use the truth of the statement being proved (or something equivalent) in the proof itself.

Example:

- Conjecture: *if n^2 is even then n is even.*
- Proof: If n^2 is even then $n^2 = 2k$ for some k. Let $n = 2l$ for some l. Hence, x must be even.

(Note that the statement $n = 2l$ is introduced without any argument showing it.)

Methods of Proof

- Direct Proof
- Proof by Contraposition
- Proof by Contradiction
- Proof of Equivalences
- Proof by Cases
- Existence Proofs
- Counterexamples