THU JAN, 30 (cont.)

The Foundations: Logic and Proofs

Chapter 1, Part III: Proofs

1

Rules of Inference

Section 1.6

2

Section Summary

- Valid Arguments
- Inference Rules for Propositional Logic
- Using Rules of Inference to Build Arguments
- Rules of Inference for Quantified Statements
- Building Arguments for Quantified Statements

3

four logical form

1. Modus Pones
2. Modus Tollens
3. Hypothetical Syllogism
4. Disjunctive Syllogism
5. Simplification
6. Universal Instantiation
7. Universal Generalization

Revisiting the Socrates Example

- We have the two premises:
  - "All men are mortal."
  - "Socrates is a man."
- And the conclusion:
  - "Socrates is mortal."
- How do we get the conclusion from the premises?

4

domain should be stated clearly

For instance, the domain of men here is all human being

Also an example of modus ponus

The Argument

- We can express the premises (above the line) and the conclusion (below the line) in predicate logic as an argument:

$$\frac{\forall x(Man(x) \rightarrow Mortal(x)) \qquad Man(Socrates)}{\therefore \quad Mortal(Socrates)}$$

- We will see that this is a valid argument.

5

Formal version using predicate

Modus ponens

Valid Arguments

- We will show how to construct valid arguments in two stages; first for propositional logic and then for predicate logic. The rules of inference are the essential building block in the construction of valid arguments.
  1. Propositional Logic
     Inference Rules
  2. Predicate Logic
     Inference rules for propositional logic plus additional inference rules to handle variables and quantifiers.

6

if u set up a premises and used the correct

logic then it is a valid argument

Arguments in Propositional Logic

- An *argument* in propositional logic is a sequence of propositions. All but the final proposition are called *premises*. The last statement is the *conclusion*.
- The argument is valid if the premises imply the conclusion. An *argument form* is an argument that is valid no matter what propositions are substituted into its propositional variables.
- If the premises are $p_1, p_2, \ldots, p_n$ and the conclusion is q then
  $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$ is a tautology.
- Inference rules are all simple argument forms that will be used to construct more complex argument forms.

7

Rules of Inference for Propositional Logic: Modus Ponens

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

Corresponding Tautology:
$(p \wedge (p \rightarrow q)) \rightarrow q$

Example:
Let p be "It is snowing."
Let q be "I will study discrete math."

"If it is snowing, then I will study discrete math."
"It is snowing."

"Therefore , I will study discrete math."

8

Modus Ponens start with an implication

Common mistake: add stuff that doesn't matter

Method that affirms

Modus Tollens

$$\begin{array}{l} p \rightarrow q \\ \neg q \\ \hline \therefore \neg p \end{array}$$

Corresponding Tautology:
$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$

Example:
Let p be "it is snowing."
Let q be "I will study discrete math."

"If it is snowing, then I will study discrete math."
"I will not study discrete math."

"Therefore , it is not snowing."

9

Method that denies things

End of WED

Hypothetical Syllogism (transitivity of →)

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$$

Corresponding Tautology:
$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$
If p implies q and q implies r, then p implies r

Example:
Let p be "it snows."
Let q be "I will study discrete math."
Let r be "I will get an A."

"If it snows, then I will study discrete math."
"If I study discrete math, I will get an A."

"Therefore , If it snows, I will get an A."

10

Skipped

Disjunctive Syllogism

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

Corresponding Tautology:
$(\neg p \wedge (p \vee q)) \rightarrow q$

Example:
Let p be "I will study discrete math."
Let q be "I will study English literature."

"I will study discrete math or I will study English literature."
"I will not study discrete math."

"Therefore , I will study English literature."

11

Skipped

Addition

$$\begin{array}{l} p \\ \hline \therefore p \vee q \end{array}$$

Corresponding Tautology:
$p \rightarrow (p \vee q)$

Example:
Let p be "I will study discrete math."
Let q be "I will visit Las Vegas."

"I will study discrete math."

"Therefore, I will study discrete math or I will visit Las Vegas."

12

Skipped

Simplification

$$\frac{p \wedge q}{\therefore q}$$

Corresponding Tautology:
$(p \wedge q) \rightarrow p$

Example:
Let p be "I will study discrete math."
Let q be "I will study English literature."

"I will study discrete math and English literature"

"Therefore, I will study discrete math."

13

Skipped

Conjunction

$$\frac{p}{q}$$
$$\therefore p \wedge q$$

Corresponding Tautology:
$((p) \wedge (q)) \rightarrow (p \wedge q)$

Example:
Let p be "I will study discrete math."
Let q be "I will study English literature."

"I will study discrete math."
"I will study English literature."

"Therefore, I will study discrete math and I will study English literature."

14

Skipped

Resolution

Resolution plays an important role in AI and is used in Prolog.

$$\frac{\neg p \vee r}{p \vee q}$$
$$\therefore q \vee r$$

Corresponding Tautology:
$((\neg p \vee r) \wedge (p \vee q)) \rightarrow (q \vee r)$

Example:
Let p be "I will study discrete math."
Let r be "I will study English literature."
Let q be "I will study databases."

"I will not study discrete math or I will study English literature."
"I will study discrete math or I will study databases."

"Therefore, I will study databases or I will study English literature."

15

Skipped

Using the Rules of Inference to Build Valid Arguments

- A *valid argument* is a sequence of statements. Each statement is either a premise or follows from previous statements by rules of inference. The last statement is called conclusion.
- A valid argument takes the following form:

S_1
S_2
.
.
.
S_n

$\therefore$ C

16

Valid Arguments

Example 1: From the single proposition

$$p \wedge (p \rightarrow q)$$

Show that q is a conclusion.

Solution:

#	Statement	Inference Rule	Uses statement(s) #
1	$p \wedge (p \rightarrow q)$	Premise	
2	p	Simplification	1
3	$p \rightarrow q$	Simplification	1
4	q	Modus ponens	3, 2

17

Valid Arguments

Example 2:

- With these hypotheses:
  "It is not sunny this afternoon and it is colder than yesterday."
  "We will go swimming only if it is sunny."
  "If we do not go swimming, then we will take a canoe trip."
  "If we take a canoe trip, then we will be home by sunset."
- Using the inference rules, construct a valid argument for the conclusion:
  "We will be home by sunset."

Solution:

1. Choose propositional variables:
   p : "It is sunny this afternoon." r : "We will go swimming." t : "We will be home by sunset."
   q : "It is colder than yesterday." s : "We will take a canoe trip."
2. Translation into propositional logic:

$$\text{Hypotheses: } \neg p \wedge q,\ r \rightarrow p,\ \neg r \rightarrow s,\ s \rightarrow t$$
$$\text{Conclusion: } t$$

Continued on next slide →

18

Valid Arguments

3. Construct the Valid Argument

Step	Reason
1. $\neg p \wedge q$	Premise
2. $\neg p$	Simplification using (1)
3. $r \rightarrow p$	Premise
4. $\neg r$	Modus tollens using (2) and (3)
5. $\neg r \rightarrow s$	Premise
6. s	Modus ponens using (4) and (5)
7. $s \rightarrow t$	Premise
8. t	Modus ponens using (6) and (7)

19

Handling Quantified Statements

- Valid arguments for quantified statements are a sequence of statements. Each statement is either a premise or follows from previous statements by rules of inference which include:
  - Rules of Inference for Propositional Logic
  - Rules of Inference for Quantified Statements
- The rules of inference for quantified statements are introduced in the next several slides.

20

Universal Instantiation (UI)

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Example: Our domain consists of all dogs and Fido is a dog.

Premise: "All dogs are cuddly."

Conclusion: "Therefore, Fido is cuddly."

21

Universal Generalization (UG)

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

Used often implicitly in Mathematical Proofs.

22

Existential Instantiation (EI)

$$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$$

Example:

"There is someone who got an A in the course."
"Let's call her *a* and say that *a* got an A"

23

Existential Generalization (EG)

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$$

Example:

"Michelle got an A in the class."
"Therefore, someone got an A in the class."

24

Using Rules of Inference

Example 1: Using the rules of inference, construct a valid argument to show that
"John Smith has two legs"
is a consequence of the premises:
"Every man has two legs." "John Smith is a man."

Solution: Let $M(x)$ denote "x is a man" and $L(x)$ "x has two legs" and let John Smith be a member of the domain.

Valid Argument:

Step	Reason
1. $\forall x(M(x) \rightarrow L(x))$	Premise
2. $M(J) \rightarrow L(J)$	UI from (1)
3. $M(J)$	Premise
4. $L(J)$	Modus Ponens using (2) and (3)

25

Using Rules of Inference

Example 2: Use the rules of inference to construct a valid argument showing that the conclusion
"Someone who passed the first exam has not read the book."
follows from the premises
"A student in this class has not read the book."
"Everyone in this class passed the first exam."

Solution: Let $C(x)$ denote "x is in this class," $B(x)$ denote "x has read the book," and $P(x)$ denote "x passed the first exam."

First we translate the premises and conclusion into symbolic form.

$$\begin{array}{l} \exists x(C(x) \wedge \neg B(x)) \\ \forall x(C(x) \rightarrow P(x)) \\ \hline \therefore\ \exists x(P(x) \wedge \neg B(x)) \end{array}$$

Continued on next slide →

26

Using Rules of Inference

Valid Argument:

Step	Reason
1. $\exists x(C(x) \wedge \neg B(x))$	Premise
2. $C(a) \wedge \neg B(a)$	EI from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$	Premise
5. $C(a) \rightarrow P(a)$	UI from (4)
6. $P(a)$	MP from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \wedge \neg B(a)$	Conj from (6) and (7)
9. $\exists x(P(x) \wedge \neg B(x))$	EG from (8)

27

Returning to the Socrates Example

$$\forall x(Man(x) \rightarrow Mortal(x))$$

$$Man(Socrates)$$

$$\therefore \quad Mortal(Socrates)$$

28

Solution for Socrates Example

Valid Argument

Step	Reason
1. $\forall x(Man(x) \rightarrow Mortal(x))$	Premise
2. $Man(Socrates) \rightarrow Mortal(Socrates)$	UI from (4)
3. $Man(Socrates)$	Premise
4. $Mortal(Socrates)$	MP from (2) and (3)

29

Universal Modus Ponens

Universal Modus Ponens combines universal instantiation and modus ponens into one rule.

$$\forall x(P(x) \rightarrow Q(x))$$
$$P(a), \text{ where } a \text{ is a particular element in the domain}$$
$$\therefore Q(a)$$

This rule could be used in the Socrates example.

30

Skipped till this point

TUE FEB 02

Introduction to Proofs

Section 1.7

31

Section Summary

- Mathematical Proofs
- Forms of Theorems
- Direct Proofs
- Indirect Proofs
  - Proof of the Contrapositive
  - Proof by Contradiction

32

Proofs of Mathematical Statements

- A *proof* is a valid argument that establishes the truth of a statement.
- In Math, CS, and other disciplines, informal proofs which are generally shorter, are usually used.
  - More than one rule of inference is often used in a step.
  - Steps may be skipped (Danger!).
  - The rules of inference used are not explicitly stated.
  - Easier for to understand and to explain to people.
  - But it is also easier to introduce errors.
- Proofs have many practical applications:
  - verification that computer programs are correct
  - establishing that operating systems are secure
  - enabling programs to make inferences in artificial intelligence
  - showing that system specifications are consistent

33

with a little modification it can be changed to one of the inferences (modus ponens)

Definitions

- A *theorem* is a statement that can be shown to be true using:
  - definitions
  - other theorems
  - *axioms* (statements which are **assumed** true)
  - rules of inference
- A *lemma* is a 'helping theorem' or a result which is needed to prove a theorem.
- A *corollary* is a theorem which follows directly from another theorem.
- Less important theorems are sometimes called *propositions*.
- A *conjecture* is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. Conjectures often turn out to be false.

34

conjecture - proposed to be true.

axiom ->

Forms of Theorems

- Many theorems assert that a property holds for all elements in a domain, such as the integers, the real numbers, or some of the discrete structures that we will study.
- Often the universal quantifier (needed for a precise statement of a theorem) is omitted by standard mathematical convention.

For example, the statement:

"If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$ "

really means

"For ***all positive*** real numbers x and y, if $x > y$, then $x^2 > y^2$."

35

are usually universal

Proving Theorems

- Many theorems have the form:
  $$\forall x(P(x) \rightarrow Q(x))$$
- To prove them, we show that, where c is an arbitrary element of the domain, $P(c) \rightarrow Q(c)$
- By universal generalization[1] the truth of the original formula follows.
- Generally, we must prove something of the form:
  $$p \rightarrow q$$

1: Universal generalization says if you can show that a certain idea is true for an ***arbitrary (i.e., unspecified)*** value in the domain of discussion, then the idea is valid for ***every*** value in the domain.

36

Universal generalization

we assume that it's value in it's domain

since i have proved it for an arbitrary value in its domain. then it must be the case for all

Proving Conditional Statements: $p \rightarrow q$

- *Trivial Proof*: If we know q is true, then $p \rightarrow q$ is true as well. (Check the truth table for $p \rightarrow q$.)
  "If it is raining then 1=1."
- *Vacuous Proof*: If we know p is false then $p \rightarrow q$ is true as well . (Check the truth table for $p \rightarrow q$.)
  "If I am both alive and dead then 2 + 2 = 5."

[Even though these examples are silly, both trivial and vacuous proofs are often used as starting points in *mathematical induction*, as you will see in a more advanced course, i.e., 2166)]

37

trivial -> dealing with 0

if the conclusion is T, then its always T. regardless of what p is

Vacuous —>

if the hypothesis is F, then the implication is always true

Even and Odd Integers

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

We will need these basic facts about the integers in some of the example proofs to follow. We will learn more about the integers when we investigate number theory.

38

Listing won't work
Provide techniques

Nodd -> N^2odd

Proving Conditional Statements: $p \rightarrow q$

- *Direct Proof*: **Assume that p is true. Use inference, axioms, and logical equivalences to show that q must also be true.**

Example:
Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."
Solution:
Assume that n is odd (i.e., assume p true): then $n = 2k + 1$ for some integer k.
Squaring both sides of the equation, we get: $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2r + 1$,
where $r = 2k^2 + 2k$, an integer (by the closure properties of the integers).
We have proved that if n is an odd integer, then n^2 is an odd integer. ◄
[◄ marks the end of the proof. **QED** (Quod Est Demonstradum Latin for "thus it is demonstrated") is sometimes used instead.]

39

assume p is T: n = 2k+1, where k EE Z

n^2 = (2k+1)^2 = (4k^2 + 4k) + 1

= 2(2k^2 + 2k) + 2….integer by the closure rule

=2(2k^2+2k)+2… the parath are integer

= 2m+1… thus m EE Z odd

Proving Conditional Statements: $p \rightarrow q$

Definition: The real number r is *rational* if there exist integers p and q with $q \neq 0$ such that $r = p/q$

Example: Prove that the sum of two rational numbers is rational.

Solution: Assume r and s are two rational numbers. Then there must be integers p, q and also t, u such that

$$r = p/q, \quad s = t/u, \quad u \neq 0, \ q \neq 0$$

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu+qt}{qu} = \frac{v}{w} \quad \text{where } v = pu + qt, \ w = qu \neq 0$$

Thus the sum is rational. QED (or ◄). Note that this proof uses the addition-subtraction algorithm for rational numbers, a theorem, and the closure properties. Since this is an informal proof, it is *assumed* that the reader recognizes this.

40

v/w .. = an integer/ an integer

Proving Conditional Statements: $p \rightarrow q$

- *Proof by Contraposition*: **Assume $\neg q$ is true and show $\neg p$ is true also**. This is an *indirect proof* method as you work with a modified version of the original theorem. If we give a direct proof of $\neg q \rightarrow \neg p$ then we have a proof of $p \rightarrow q$.

  Why does this work?
  Because the proposition and it's contrapositive are logically equivalent, if the contrapositive is true, so is the original proposition.

Example: Prove that if n is an integer and $3n + 2$ is odd, then n is odd.
Solution: Assume n is even ($\neg q$) and show $3n + 2$ is even ($\neg p$). Let $n = 2k$ for some integer k.
Then $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j$ for $j = 3k + 1$
Therefore $3n + 2$ is even. ($\neg p$) ◄
Since we have shown $\neg q \rightarrow \neg p$, then $p \rightarrow q$ must hold as well. If n is an integer and $3n + 2$ is odd (not even), then n is odd (not even).

41

p -> q…. 3m+2 odd -> n odd

contrapositive.. !q ->!p.. !(n odd)-> !(3m +2 odd)

n even -> 3n+2 even

Let, n = 2p and p EE Z

3(2p)+2 = 6p + 2 = 2(3p + 1) even… p EE Z

Proving Conditional Statements: $p \rightarrow q$

Example: Prove that for an integer n, if n^2 is odd, then n is odd.
Here: $p = n^2$ is odd $\quad\quad$ $q = n$ is odd
Solution: Use proof by contraposition: the contrapositive of the theorem is (since $\neg p = n^2$ is even and $\neg$ q = n is even) we have:
If n is even then n^2 is even.

Assume n is even (i.e., not odd). Therefore, there exists an integer k such that $n = 2k$. Hence,
$n^2 = 4k^2 = 2(2k^2)$
and n^2 is even (i.e., not odd).

We have shown that if n is an even integer, then n^2 is even. Therefore by contraposition, for an integer n, if n^2 is odd, then n is odd. **QED**

42

lets suppose that a right triangle can be drawn on a flat surface

contradict your hypothesis

example: angle with two right angle = pi/2 +pi/2 + 0

Proving Conditional Statements: $p \rightarrow q$

- *Proof by Contradiction*: (AKA *reductio ad absurdum*).
  To **prove** p, **assume** $\neg p$ **and derive a contradiction such as** $p \wedge \neg p$, (an indirect form of proof). *Since we have shown that* $\neg p \rightarrow F$ *is true , it follows that the contrapositive* $T \rightarrow p$ *also holds.*

Example: Prove that if you pick 22 days from the calendar, at least 4 must fall on the same day of the week.

Solution: Assume that no more than 3 of the 22 days fall on the same day of the week.

Because there are 7 days in a week, we could only have picked 21 days.

This contradicts the assumption that we have picked 22 days so, therefore, having picked 22 days, at least 4 days must fall on the same day of the week. ◀

43

TUE FEB 2 END

Proof by Contradiction

- **Example**: Use a proof by contradiction to show that $\sqrt{2}$ is irrational.
- In this case, we will assume that

Solution: Suppose $\sqrt{2}$ is rational. Then there exists integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ **and** a **and** b **have no common factors** (i.e., a/b is reduced to lowest terms). Then, squaring both sides:

$$2 = \frac{a^2}{b^2} \quad \text{and} \quad 2b^2 = a^2$$

Therefore a^2 must be even. If a^2 is even then a must be even (a previous exercise). Since a is even, $a = 2c$ for some integer c. Thus,

$$2b^2 = 4c^2 \qquad b^2 = 2c^2$$

Therefore b^2 is even. So, b must be even as well.

But then 2 must divide both a and b. **This contradicts our assumption that** a **and** b **have no common factors**. We have proved by contradiction that our initial assumption must be false and therefore $\sqrt{2}$ is irrational . ◀

44

Proof by Contradiction

- **Example**: Prove that there is no largest prime number.

Solution: *Assume that there is a largest prime number*. Call it p_n. Hence, we can make a list of all the primes: 2, 3, 5, 7, 11, 13, ..., p_n.

Form $r = p_1 \times p_2 \times \ldots \times p_n + 1$

By inspection, none of the prime numbers on the list divides r. Therefore, either r is prime and $r > p_n$ or there is a smaller prime (i.e. a prime $p_s < p_n$) that divides r.[1] This contradicts the assumption that there is a largest prime: either $r > p_n$ or, if r is not prime, recompute r by including p_s, then repeat the argument. Therefore, there is no largest prime. ◀

1. **Fundamental Theorem of Arithmetic**: Every positive integer ≥ 2 is either a prime or the product of primes and such product is unique up to the order of the factors. E.g., 17 is prime; 34 is composite, i.e., 34 = 2 * 17

45

Theorems that are Biconditional Statements

- **To prove a theorem that is a biconditional** statement, that is, a statement of the form $p \leftrightarrow q$, **we must show that $p \rightarrow q$ and $q \rightarrow p$ are both true.**

Example: Prove the theorem: "If n is an integer, then n is odd if and only if n^2 is odd."

Solution: We have already shown (in previous examples) that both $p \rightarrow q$ and $q \rightarrow p$, we can therefore conclude that $p \leftrightarrow q$.

Frequently *iff*" is used as an abbreviation for "if an only if," as in

If n is an integer, then n is odd *iff*" n^2 is odd.

46

What is wrong with this?

"Proof" that $1 = 2$

Step	Reason
1. $a = b$	Premise
2. $a^2 = a \times b$	Multiply both sides of (1) by a
3. $a^2 - b^2 = a \times b - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Algebra on (3)
5. $a + b = b$	Divide both sides by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$
7. $2 = 1$	Divide both sides of (6) by b

Solution: Steps 4 & 5: a – b = 0 by the premise $a = b$ and division by 0 is undefined.

47

Looking Ahead

- If direct methods of proof do not work:
  - We may need a clever use of a proof by contraposition.
  - Or a proof by contradiction.
  - In the next section, we will see strategies that can be used when straightforward approaches do not work.
  - In Chapter 6, we will see combinatorial proofs.
  - Proof by Induction, while not covered here (covered in CIS 2166), is a very important technique, particularly in CS for analyzing recursive algorithms.

48

THU FEB 6

Proof Methods and Strategy

Section 1.8

49

Section Summary

- Proof by Exhaustion and by Cases
- Existence Proofs
  - Constructive
  - Nonconstructive
- Disproof by Counterexample
- Nonexistence Proofs
- Uniqueness Proofs
- Proof Strategies
- Proving Universally Quantified Assertions
- Open Problems

50

Proof by Exhaustion

- No, this doesn't mean keep trying until you are too tired to continue and declare the theorem proved just to finish—it does mean to make a proof by examining ALL possible combinations of elements of the domain and showing that the theorem holds for ALL of them.
- This also means that proving a theorem by exhaustion is not possible when the domain is an infinite set and is an intractable problem if the cardinality of the domain is very large.
- The main form of error here is to "prove" that a conjecture is true for a subset of a few elements chosen from the domain and ignoring the rest of the (possibly infinite) set.

PROOF BY EXAMPLE IS NOT A PROOF

51

a proof made by doing every possible combination

Usually when the domain is small

Proof by Exhaustion

- This form of proof applies ONLY when the size of the domain of the predicate is sufficiently small that each possible choice of domain element(s) can be tested.
- Consider, e.g.: Show (i.e., prove) that no 4^{th} power of an integer x such that $1 \le x \le 5$ is the sum of two other such values:
- In this case, the domain set is {1, 2, 3, 4, 5} and the set of 4^{th} powers is {1, 16, 81, 256, 625}. Adding the powers in pairs yields: 1+1=2, 1+16=17, 1+81=82, 1+256=257, 1+625=626; 16+16=32, 16+81=97,16+256=272, 16+625=641; 81+256=337, 81+625=706; 256+625=881. The result follows from an inspection of the sums (which is a **complete set of all of the possibilities**). This is intractable if the number of cases is large, say if the domain was $0 \le x \le 1{,}000{,}000{,}000$.
- REMEMBER: *Proof by example is NOT proof unless you investigate EVERY POSSIBLE example.*

52

proof by example is not a proof; list all possible comb

Proof by Cases

- To prove a conditional statement of the form:

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$$

- Use the tautology

$$[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$$

- Each of the implications $p_i \rightarrow q$ is a *case*.

53

Text

Proof by Cases

Example: Let $a \,@\, b = \max\{a, b\} = a$ if $a \ge b$, otherwise $a \,@\, b = \max\{a, b\} = b$.
Show that for all real numbers a, b, c

$$(a \,@\, b) \,@\, c = a \,@\, (b \,@\, c)$$

(This means the operation @ is associative.)
Proof: Let a, b, and c be arbitrary real numbers.
Then one of the following 6 cases must hold.

1. $a \ge b \ge c$
2. $a \ge c \ge b$
3. $b \ge a \ge c$
4. $b \ge c \ge a$
5. $c \ge a \ge b$
6. $c \ge b \ge a$

Continued on next slide →

54

proving it has associative property

When you take each possible case and prove them

only when the possibilities are small

Proof by Cases

Case 1: a ≥ b ≥ c

(a @ b) = a, a @ c = a, b @ c = b

Hence (a @ b) @ c = a = a @ (b @ c)

Therefore the equality holds for the first case.

A complete proof requires that the equality be shown to hold for all 6 cases. The proofs of the remaining cases are similar. *Try them yourself.*

55

Without Loss of Generality

Example: Show that if *x* and *y* are integers and both *x*·*y* *and* *x*+*y* are even, then both *x* and *y* are even.

Proof: Use a proof by contraposition. Suppose *x* and *y* are not both even. Then, one or both are odd. Without loss of generality, assume that *x* is odd. Then $x = 2m + 1$ for some integer *m*.

Case 1: y is even. Then $y = 2n$ for some integer *n*, so $x + y = (2m + 1) + 2n = 2(m + n) + 1$ is odd.

Case 2: y is odd. Then $y = 2n + 1$ for some integer *n*, so $x \cdot y = (2m + 1)(2n + 1) = 2(2m \cdot n + m + n) + 1$ is odd. ◀

We only cover the case where *x* is odd because the case where *y* is odd is similar (in this case, virtually identical—just interchange *x* and *y*. The use of the phrase *without loss of generality* (WLOG) indicates this.

56

Existence

Existence Proofs

Srinivasa Ramanujan (1887-1920)

- Proof of theorems of the form $\exists x P(x)$.
- **Constructive** existence proof:
  - Find an explicit value of *c*, for which *P(c)* is true.
  - Then $\exists x P(x)$ is true by Existential Generalization (EG).

Example: Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways:

Proof: 1729 is such a number since

$1729 = 10^3 + 9^3 = 12^3 + 1^3$ ◀

Godfrey Harold Hardy (1877-1947)

57

Constructive— u present the answer to the existence proof

Nonconstructive Existence Proofs

- In a ***nonconstructive* existence proof, assume no *c* exists which makes *P(c)* true and derive a contradiction.**

Example: Show that there exist irrational numbers x and y such that x^y is rational.

Proof: We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. If it is rational, we have two irrational numbers x and y with x^y rational, namely $x = \sqrt{2}$ and $y = \sqrt{2}$. But if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ so that $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\sqrt{2})} = \sqrt{2}^2 = 2$. ◀

- Note that the proof tells us that one of the two pairs of x and y must work, but doesn't actually specify which in the sense that *both* may work, but this is **not demonstrated**; therefore, the proof is **nonconstructive**.

58

Second part is made from assuming that the first part being irrational

Thus, the assumption leads it to be nonconstructive

Constructive & Nonconstructive Proofs

- Theorem: There exist distinct integers x & $y \in \{1901, 1902, \ldots, 2014\}$ such that the last two digits of x^2 and y^2 are the same.
- **Nonconstructive proof**: There are 114 distinct integers in the given set (elements), but only 100 combinations of last two digits, i.e., {00, …, 99} (categories). Because 114 elements are assigned to only 100 categories, there must be at least one category with more than one element {which shows such numbers MUST exist, but doesn't name any, hence this is a nonconstructive proof. N.B.: this is an example of the "pigeon hole principle" we will study soon}
- **Constructive proof:** Let $x = 1986$ and $y = 1964$. Since $x^2 = 3{,}944{,}196$ and $y^2 = 3{,}857{,}296$, both have 96 as their last 2 digits and the theorem is satisfied.

59

NonConstructive - I can demonstrate that there is an answer pigeon hole principal

Disproof by Counterexample

- Recall $\exists x \neg P(x) \equiv \neg \forall x P(x)$
- To establish that $\neg \forall x P(x)$ is true (or $\forall x P(x)$ is false) find a c such that $\neg P(c)$ is true or $P(c)$ is false.
- In this case c is called a *counterexample* to the assertion $\forall x P(x)$.
- Note: while only an exhaustive examination of all possibilities (Proof by Cases) or logical deduction can prove a conjecture TRUE, a single counterexample is sufficient to show a *universal* conjecture $(\forall x P(x))$ is FALSE.

Example: Conjecture: "*Every positive integer is the sum of the squares of 3 integers.*" The integer 7 is a counterexample: $1^2+1^2+2^2=6$ and $1^2+2^2+2^2=9$ and these examples are as close as you can come to a sum of 7…so the conjecture is false.

60

The number 7 is a counterexample

Foundation of Mathematical models

Existance & Uniqueness Proofs

- Some theorems assert the existence of a unique element with a particular property, $\exists!x\, P(x)$. The two parts of an existence *uniqueness proof* are:
  - ***Existence***: We show that an element x with the property exists.
  - ***Uniqueness***: We show that if $y \neq x$, then y does not have the property.

Example: Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Solution:

- **Existence**: The real number $r = -b/a$ is a solution of $ar + b = 0$ because $a(-b/a) + b = -b + b = 0$.
- **Uniqueness**: Suppose that s is a real number such that $as + b = 0$. Then $ar + b = as + b$, where $r = -b/a$. Subtracting b from both sides and dividing by a shows that $r = s$. ◀

61

to prove existence. Lets assume another answer exist

An Important Existence and Uniqueness Theorem in ODE

- Let R be a rectangular region in the ty-plane defined by $t \in [a, b]$ *and* $y \in [c, d]$ that contains the point (t_0, y_0) in its interior. If $f(t, y)$ and $\frac{\partial f}{\partial y}$ are continuous on R, then there exists some interval I_0: $t_0 - h < t < t_0 + h, h > 0$ contained in [a,b] and a *unique* function $y(t)$ defined on I_0 that is a solution of the Initial Value Problem: solve $\frac{dy}{dt} = f(t, y)$ subject to $y(t_0) = y_0$.

62

Proof Strategies for showing $p \rightarrow q$

- Choose a method.
  1. First try a direct method of proof.
  2. If this does not work, try an indirect method (e.g., try to prove the contrapositive or try contradiction).
- For whichever method you are trying, choose a strategy.
  1. First try *forward reasoning*. Start with the axioms and known theorems and construct a sequence of steps that end in the conclusion. Start with p and prove q, or start with $\neg q$ and prove $\neg p$.
  2. If this doesn't work, try *backward reasoning*. When trying to prove q, find a statement p that we can prove with the property $p \rightarrow q$.

63

what do I know about it

Direct Proof

Either contrapositive or contradiction

Start from the conclusion to the hypothesis

Backward Reasoning

Example: Suppose that two people play a game taking turns removing, 1, 2, or 3 stones at a time from a pile that begins with 15 stones. The person who removes the last stone wins the game. Show that the first player can win the game no matter what the second player does.

Proof: Let *n* be the last step of the game.

Step n: Player$_1$ can win if the pile contains 1,2, or 3 stones.

Step n-1: Player$_2$ will have to leave such a pile if the pile that he/she is faced with has 4 stones.

Step n-2: Player$_1$ can leave 4 stones when there are 5,6, or 7 stones left at the beginning of his/her turn.

Step n-3: Player$_2$ must leave such a pile, if there are 8 stones .

Step n-4: Player$_1$ has to have a pile with 9,10, or 11 stones to ensure that there are 8 left.

Step n-5: Player$_2$ needs to be faced with 12 stones to be forced to leave 9,10, or 11.

Step n-6: Player$_1$ can leave 12 stones by removing 3 stones.

Now reasoning forward, the first player can ensure a win (as long as they don't make a mistake) by removing 3 stones and leaving 12, etc.

64

Universally Quantified Assertions

- To prove theorems of the form $\forall x P(x)$, assume *c* is an *arbitrary* member of the domain and show that *P*(*c*) must be true. Using Universal Generalization it follows that $\forall x P(x)$.

Example: An integer *x* is even if and only if x^2 is even.

Solution: The quantified assertion is

$\forall x$ [*x* is even $\leftrightarrow$ x^2 is even]

We assume *x* is arbitrary.

Recall that $p \leftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$

So, we have two cases to consider. These are considered in turn.

Continued on next slide →

65

Universally Quantified Assertions

Case 1. We show that if *x* is even then x^2 is even using a direct proof (the *only if* part or *necessity*).

If *x* is even then $x = 2k$ for some integer *k*.

Hence $x^2 = 4k^2 = 2(2k^2)$ which is even since it is an integer divisible by 2.

This completes the proof of case 1.

Case 2 on next slide →

66

Universally Quantified Assertions

Case 2. We show that if x^2 is even then x must be even (the *if* part or *sufficiency*). We use a proof by contraposition.

Assume x is not even and then show that x^2 is not even.

If x is not even then it must be odd. So, $x = 2k + 1$ for some k. Then $x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

which is odd and hence not even. This completes the proof of case 2.

Since x was arbitrary, the result follows by Universal Generalization.

Therefore we have shown that x is even if and only if x^2 is even.◀

67

The Role of Open Problems

- Unsolved problems have motivated much work in mathematics. Fermat's Last Theorem was conjectured more than 300 years ago. It has only recently (1990's) been finally solved. The solution required the development of much new mathematics and proofs of conjectures thought to be unprovable.

Fermat's Last Theorem: The equation $x^n + y^n = z^n$ has no solutions in positive integers x, y, and z, whenever n is an integer, $n > 2$.

A proof was found by Andrew Wiles (Cambridge) in 1995 (final version), some 358 years after the theorem was proposed.

72

An Open Problem

- **The $3x + 1$ Conjecture**: Let T be the transformation that sends an even integer x to $x/2$ and an odd integer x to $3x + 1$; i.e., $T(x) = \begin{cases} \frac{x}{2}, x \text{ even} \\ 3x+1, x \text{ odd} \end{cases}$ for all positive integers x.

When we repeatedly apply the transformation T, we will eventually reach the integer 1.

For example, starting with $x = 13$:

$T(13) = 3 \cdot 13 + 1 = 40, T(40) = 40/2 = 20, T(20) = 20/2 = 10,$
$T(10) = 10/2 = 5, T(5) = 3 \cdot 5 + 1 = 16, T(16) = 16/2 = 8,$
$T(8) = 8/2 = 4, T(4) = 4/2 = 2, T(2) = 2/2 = 1$

The conjecture has been verified using computers up to about $1.15\ldots \cdot 10^{18}$ ($87 * 2^{60}$; reported in 2017).

73

Additional Proof Methods

- Later we will see many other proof methods:
  - Mathematical induction, which is a useful method for proving statements of the form $\forall n\, P(n)$, where the domain consists of all positive integers (CIS 2166)
  - Structural induction, which can be used to prove such results about recursively defined sets.
  - Cantor diagonalization is used to prove results about the size of infinite sets.
  - Combinatorial proofs use counting arguments (coming soon!).

74