Discrete Mathematics

離 散 數 學

江 振 國

The Foundations: Logic and Proofs

Chapter 1, Part III: Proofs

Summary

- Valid Arguments and Rules of Inference
- Proof Methods
- Proof Strategies

Rules of Inference

Section 1.6

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

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?

The Argument

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

$$\begin{array}{rl} & \forall x(Man(x) \rightarrow Mortal(x)) \\ & Man(Socrates) \\ \hline \therefore & Mortal(Socrates) \end{array}$$

- We will see shortly that this is a valid argument.

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.

Arguments in Propositional Logic

- A *argument* in propositional logic is a sequence of propositions. All but the final proposition are called *premises*. The last statement is the *conclusion*.
- An argument is valid if the truth of all its premises imply that the conclusion is true.
- A *argument form* in propositional logic is a sequence of compound propositions involving propositional variables.
  - An argument form is valid no matter which particular propositions are substituted for the propositional variables in its premises.
  - The conclusion is true if the premises are all true.

Using Truth Table

- Determine whether this argument is valid by using a truth table:
  - I play golf or tennis.
  - If it is not Sunday, I play golf and tennis.
  - If it is Saturday or Sunday, then I don't play golf.
  - Therefore, I don't play golf.
- Using the variables:
  - g: I play golf
  - t: I play tennis
  - s: it is Saturday
  - u: it is Sunday,

Using Truth Table

- the argument can be written in symbols as:
  - g ∨ t
  - ¬u → (g ∧ t)
  - (s ∨ u)→¬g
  - ----------------
  - ¬g

g	t	s	u	$g \vee t$	$\neg u \to (g \wedge t)$	$(s \vee u) \to \neg g$	$\neg g$
T	T	T	T	T	T	F	F
T	T	T	F	T	T	F	F
T	T	F	T	T	T	F	F
T	T	F	F	T	T	T	F
T	F	T	T	T	T	F	F
T	F	T	F	T	F	F	F
T	F	F	T	T	T	F	F
T	F	F	F	T	F	T	F
F	T	T	T	T	T	T	T
F	T	T	F	T	F	T	T
F	T	F	T	T	T	T	T
F	T	F	F	T	F	T	T
F	F	T	T	F	T	T	T
F	F	T	F	F	F	T	T
F	F	F	T	F	T	T	T
F	F	F	F	F	F	T	T

In the fourth row the three hypotheses (columns 5, 6, 7) are true and the conclusion is false. Therefore, the argument is not valid.

Arguments in Propositional Logic

- From the definition of a valid argument form, the argument form with premises $p_1, p_2, \ldots, p_n$ and the conclusion is q is valid, when

  $(p_1 \land p_2 \land \ldots \land p_n) \rightarrow q$ is a tautology.
- Inference rules are all arguments. Simple argument forms that will be used to construct more complex argument forms.

Rules of Inference for Propositional Logic: Modus Ponens

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

Corresponding Tautology:

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

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."

Modus Tollens

$$\begin{array}{c} p \to q \\ \neg q \\ \hline \therefore \neg p \end{array}$$

Corresponding Tautology:

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

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."

Hypothetical Syllogism

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

Corresponding Tautology:

$((p \to q) \land (q \to r)) \to (p \to r)$

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."

Disjunctive Syllogism

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

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."

Addition

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

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 Vegas.”

Simplification

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

Corresponding Tautology:

$(p \wedge q) \rightarrow q$

Example:

Let p be "I will study discrete math."

Let q be "I will study English literature."

"I will study discrete math and English literature"

"Therefore, I will study discrete math."

Conjunction

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

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."

Resolution

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

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 English literature."

Rules of Inference

Tautology	Name
$(p \land (p \rightarrow q)) \rightarrow q$	Modus ponens
$(\neg q \land (p \rightarrow q)) \rightarrow \neg p$	Modus tollens
$((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$(\neg p \land (p \lor q)) \rightarrow q$	Disjunctive syllogism
$p \rightarrow (p \lor q)$	Addition
$(p \land q) \rightarrow q$	Simplification
$((p) \land (q)) \rightarrow (p \land q)$	Conjunction
$((\neg p \lor r) \land (p \lor q)) \rightarrow (q \lor r)$	Resolution

Valid Arguments

Example 1: From the single proposition

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

Show that q is a conclusion.

Solution:

Step	**Reason**
1. $p \wedge (p \to q)$	Premise
2. p	Conjunction using (1)
3. $p \to q$	Conjunction using (1)
4. q	Modus Ponens using (2) and (3)

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

Valid Arguments

3. Construct the Valid Argument

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

Valid Arguments

- Show that the premises "If you send me an e-mail message, then I will finish writing the program," "If you do not send me an e-mail message, then I will go to sleep early," and "If I go to sleep early, then I will wake up feeling refreshed" lead to the conclusion "If I do not finish writing the program, then I will wake up feeling refreshed."

Valid Arguments

Solution: Let p be the proposition "You send me an e-mail message," q the proposition "I will finish writing the program," r the proposition "I will go to sleep early," and s the proposition "I will wake up feeling refreshed."

Then the premises are $p \to q, \neg p \to r$, and $r \to s$. The desired conclusion is $\neg q \to s$.

This argument form shows that the premises lead to the desired conclusion.

Step	**Reason**
1. $p \to q$	Premise
2. $\neg q \to \neg p$	Contrapositive of (1)
3. $\neg p \to r$	Premise
4. $\neg q \to r$	Hypothetical syllogism using (2) and (3)
5. $r \to s$	Premise
6. $\neg q \to s$	Hypothetical syllogism using (4) and (5)

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.

Universal Instantiation (UI)

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

Example:

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

“All dogs are cuddly.”

“Therefore, Fido is cuddly.”

Universal Generalization (UG)

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

Used often implicitly in Mathematical Proofs.

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”

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."

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)

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.

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

Continued on next slide →

Using Rules of Inference

Valid Argument:

Step	**Reason**
1. $\exists x(C(x) \land \neg B(x))$	Premise
2. $C(a) \land \neg B(a)$	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. $P(a) \land \neg B(a)$	Conj from (6) and (7)
9. $\exists x(P(x) \land \neg B(x))$	EG from (8)

Returning to the Socrates Example

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

$$Man(Socrates)$$

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

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)

Universal Modus Ponens

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

$$\begin{array}{l} \forall x(P(x) \to Q(x)) \\ P(a), \text{where } a \text{ is a particular} \\ \quad \text{element in the domain} \\ \hline \therefore Q(a) \end{array}$$

This rule could be used in the Socrates example.

超人範例

- 倘若超人能夠並願意防止邪惡，他就會這樣做。如果超人不能防止邪惡，那他就是無能的;如果他不願意防止邪惡，那他就是壞心腸的。我們知道，超人並沒有防止邪惡。如果超人是存在的，則他既非無能亦非壞心腸。因此，超人並不存在。

證明

1. $A \wedge W \rightarrow P$, **Premises**
2. $\neg A \rightarrow I$, **Premises**
3. $\neg W \rightarrow M$, **Premises**
4. $\neg P$, **Premises**
5. $E \rightarrow \neg \wedge \neg M$, **Premises**
6. $\neg A \vee \neg W$ from 1, 4, **Modus Tollens**
7. $A \vee I$ from 2, **Propositional Equivalences**
8. $\neg W \vee I$ from 6,7, **Resolution**
9. $W \vee M$ from 3, **Propositional Equivalences**
10. $M \vee I$ from 8,9, **Resolution**
11. $\neg(\neg M \wedge \neg I)$ from 10, **Propositional Equivalences – De Morgan**
12. $\neg E$ from 5,11, **Modus Tollens**

Normal Forms

Section 1.7

Introduction to Proofs

Section 1.8

Section Summary

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

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 generally used.
  - More than one rule of inference are often used in a step.
  - Steps may be skipped.
  - 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

Definitions

- A *theorem* is a statement that can be shown to be true using:
  - definitions
  - other theorems
  - *axioms* (statements which are given as true) (原理)
  - rules of inference
- A *lemma* is a ‘helping theorem’ or a result which is needed to prove a theorem.
- A *corollary* (推論) is a result which follows directly from a theorem.
- Less important theorems are sometimes called *propositions*.
- A *conjecture* (推測) is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. It may turn out to be false.

Forms of Theorems

- 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 $x^2 > y^2$

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 the truth of the original formula follows.
- So, we must prove something of the form:

$$p \rightarrow q$$

Proving Conditional Statements: $p \rightarrow q$

- *Trivial Proof* : If we know q is true, then

  $p \rightarrow q$ is true as well.

"If it is raining then 1=1."

- *Vacuous Proof* : If we know p is false then

  $p \rightarrow q$ is true as well.

"If I am both rich and poor then $2 + 2 = 5$."

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.

Proving Conditional Statements: $p \rightarrow q$

- ***Direct Proof***: Assume that p is true. Use rules of 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. Then $n = 2k + 1$ for an 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.

We have proved that if n is an odd integer, then n^2 is an odd integer.

◀

Proving Conditional Statements: $p \rightarrow q$

Definition: The real number r is *rational* if there exist integers p and q where $q \neq 0$ 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

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

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu} = \frac{v}{w}$$

where $v = pu + qt$

$w = qu \neq 0$

Thus the sum is rational. ◀

實數系的家譜

$$\text{實數}\begin{cases}\text{有理數}\begin{cases}\text{整數}\begin{cases}\text{正整數}\\ \text{零}\\ \text{負整數}\end{cases}\\ \text{分數:有限小數, 循環小數}\end{cases}\\ \text{無理數:不循環的無限小數}\end{cases}$$

Proving Conditional Statements: $p \to q$

- ***Proof by Contraposition***: Assume $\neg q$ and show $\neg p$ is true also. This is sometimes called an *indirect proof* method. If we give a direct proof of $\neg q \to \neg p$ then we have a proof of $p \to$ q.

Example: Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

Solution: Assume n is even. So, $n = 2k$ for some integer k. Thus

$3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j$ for $j = 3k + 1$

Therefore $3n + 2$ is even. Since we have shown $\neg q \to \neg p$, $p \to q$ must hold as well. If n is an integer and $3n + 2$ is odd (not even) , then n is odd (not even).

Proving Conditional Statements: $p \to q$

Example: Prove that for an integer n, if n^2 is odd, then n is odd.

Solution: Use proof by contraposition. 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. ◀

Proving Statements $p \to q$

- ***Proof by Contradiction***:

  1. To prove p, we assume $\neg p$ is true and derive a contradiction.

  2. To prove $p \to q$, we assume both p and $\neg q$ are true. Then we should derive that $\neg p$ is also true. This leads to a contradiction.

  3. We can also assume both p and $\neg q$ are true and showing q must be also true to provide the contradiction.

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

Solution: Assume that no more than 3 of the 22 days fall on the same day of the week ($\neg q$ and assume p). Because there are 7 days of the week, we could only have picked 21 days($\neg$p). This contradicts the assumption that we have picked 22 days. ◀

Proof by Contradiction

- **Example**: Use a proof by contradiction to give a proof that $\sqrt{2}$ is irrational.

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 (see Chapter 4). Then

$$2 = \frac{a^2}{b^2} \qquad 2b^2 = a^2$$

Therefore a^2 must be even. If a^2 is even then a must be even (an 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. Again then 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 .

◀

Proof by Contradiction

- Give a proof by contradiction of the theorem “If 3n + 2 is odd, then n is odd.”
- Solution: Let *p* be “3n + 2 is odd” and *q* be “n is odd.”
  - To construct a proof by contradiction, assume that both p and ¬q are true. That is, assume that 3n + 2 is odd and that n is not odd.
  - Because n is not odd, n = 2k.
  - This implies that 3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1). It is even.
  - Because both p and ¬p are true, we have a contradiction. This completes the proof by contradiction, proving that if 3n + 2 is odd, then n is odd.

Proving Biconditional Statements

- To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we 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 (previous slides) that both $p \rightarrow q$ and $q \rightarrow p$. Therefore we can conclude $p \leftrightarrow q$.

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: Step 5. a - b = 0 by the premise and division by 0 is undefined.

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 5, we will see mathematical induction and related techniques.
  - In Chapter 6, we will see combinatorial proofs

Proof Methods and Strategy

Section 1.9

Section Summary

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

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*.

Proof by Cases

Example: Let a @ b = max{a, b} = a if $a \geq b$, 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. $a \geq b \geq c$
2. $a \geq c \geq b$
3. $b \geq a \geq c$
4. $b \geq c \geq a$
5. $c \geq a \geq b$
6. $c \geq b \geq a$

Continued on next slide →

Proof by Cases

Case 1: $a \geq b \geq c$

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

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. But the proofs of the remaining cases are similar. Try them. ◄

Without Loss of Generality

Example: Show that if x and y are integers and both $x{\cdot}y$ *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 k.

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. The use phrase ***without loss of generality*** (WLOG) indicates this.

Existence Proofs

- 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

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

◀

Nonconstructive Existence Proofs

- In a *nonconstructive* existence proof, we do not find an element c such that P(c) is true, but rather prove that $\exists x\, P(x)$ is true in some other way.
- One common method of giving a nonconstructive existence proof is to use proof by contradiction and show that the negation of the existential quantification implies a contradiction.

Nonconstructive Existence Proofs

- **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 $y = \sqrt{2}$.

If $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ so that $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\sqrt{2})} = \sqrt{2}^{2} = 2$. ◀

This is a example of nonconstructive existence proof because we have not found irrational number x and y such that xy is rational. Rather, we have shown either the pair $x = \sqrt{2}$ and $y = \sqrt{2}$ or $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ have the desired property, but we do not know which pair works!

Counterexamples

- 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 $\forall x P(x)$.

Example: "Every positive integer is the sum of the squares of 3 integers." The integer 7 is a counterexample. So the claim is false.

Uniqueness Proofs

- Some theorems asset the existence of a unique element with a particular property, $\exists! x\, P(x)$. The two parts of a *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 $r = s$. ◀

Proof Strategies for proving $p \rightarrow q$

- 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).
- 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 $p \rightarrow q$.

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 by removing 3 stones and leaving 12.

Universally Quantified Assertions

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

  $\forall x\, [x \text{ is even} \leftrightarrow x^2 \text{ is even}]$

  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 →

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 →

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.

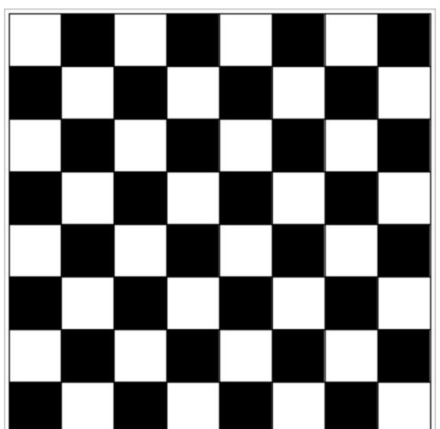
Since x was arbitrary, the result follows by UG.

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

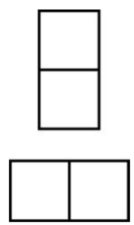
Proof and Disproof: Tilings

Example 1: Can we tile the standard checkerboard using dominos?

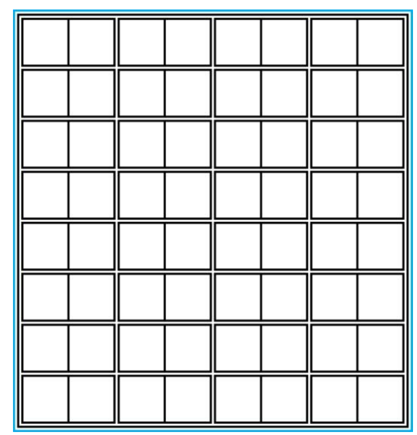
Solution: Yes! One example provides a constructive existence proof.



The Standard Checkerboard



Two Dominoes



One Possible Solution

Tilings

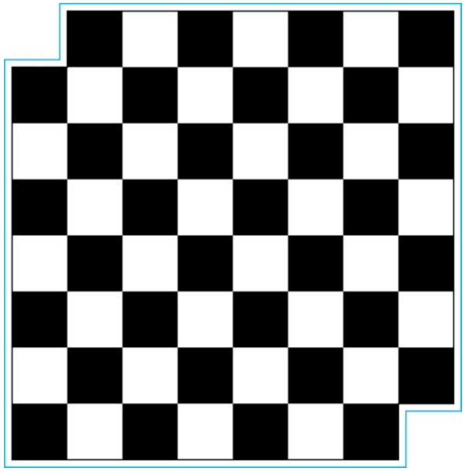
Example 2: Can we tile a checkerboard obtained by removing one of the four corner squares of a standard checkerboard?

Solution:

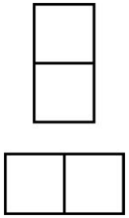
- Our checkerboard has $64 - 1 = 63$ squares.
- Since each domino has two squares, a board with a tiling must have an even number of squares.
- The number 63 is not even.
- We have a contradiction. ◀

Tilings

Example 3: Can we tile a board obtained by removing both the upper left and the lower right squares of a standard checkerboard?



Nonstandard Checkerboard



Dominoes

Continued on next slide →

Tilings

Solution:

- There are 62 squares in this board.
- To tile it we need 31 dominos.
- *Key fact*: Each domino covers one black and one white square.
- Therefore the tiling covers 31 black squares and 31 white squares.
- Our board has either 30 black squares and 32 white squares or 32 black squares and 30 white squares.
- Contradiction! ◀

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 been finally solved.

Fermat's Last Theorem: The equation $x^n + y^n = z^n$ has no solutions in integers x, y, and z, with $xyz \neq 0$ whenever n is an integer with $n > 2$.

A proof was found by Andrew Wiles in the 1990s.

An Open Problem

- **The 3*x* + 1 Conjecture**: Let T be the transformation that sends an even integer x to $x/2$ and an odd integer x to $3x + 1$. 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 for all integers using computers up to $5.6 \cdot 10^{13}$.

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.
  - 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.