Discrete Mathematics

Chapter 1, Part III: Proofs

Reference book: Discrete Mathematics and Its Applications 8th ed. (Rosen, 2019)

Rules of Inference

Section 1.6

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:

$$\forall x\left(Man\left(x\right)\rightarrow Mortal\left(x\right)\right)$$
$$Man\left(Socrates\right)$$
$$\therefore \quad Mortal\left(Socrates\right)$$

We will see shortly that this is a valid argument.

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*.

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.

Argument form with premises $p_1, p_2, \ldots, p_n$ and conclusion q is valid when $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$ is a tautology.

Inference rules are simple argument forms that will be used to construct more complex argument forms.

Rules of Inference for Propositional Logic: Modus Ponens

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

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

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

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:

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

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

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

Corresponding Tautology:

$$\left(\neg p \wedge \left(p \vee q\right)\right) \rightarrow q$$

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

Las Vegas.”

Simplification

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

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.”

Conjunction

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

Corresponding Tautology:

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

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

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

Corresponding Tautology:

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

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.”

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

$\therefore C$

Valid Arguments 2

Example 1: From the single proposition

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

Show that q is a conclusion.

Solution:

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

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 1

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. $\forall x\left(M\left(x\right)\rightarrow L\left(x\right)\right)$	Premise
2. $M\left(J\right)\rightarrow \mathrm{L}\left(J\right)$	UI from $\left(1\right)$
3. $M\left(J\right)$	Premise
4. $L\left(J\right)$	Modus Ponens using $\left(2\right)$ and $\left(3\right)$

Returning to the Socrates Example

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

$$\frac{Man(Socrates)}{\therefore \quad Mortal(Socrates)}$$

Step	Reason
1. $\forall x\left(Man(x) \rightarrow Mortal(x)\right)$	Premise
2. $Man(Socrates) \rightarrow Mortal(Socrates)$	UI from (1)
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.

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

This rule could be used in the Socrates example.

Introduction to Proofs

Section 1.7

Definitions

A *theorem* is a statement that can be shown to be true using:

- definitions
- other theorems
- *axioms* (statements which are given as true)
- rules of inference

A *lemma* is a 'helping theorem' or a result which is needed to prove a theorem.

A *corollary* is a result which follows directly from a 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. It may turn out to be false.

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 in this class.

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:

$$\forall x\big(P(x) \rightarrow Q(x)\big)$$

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 though these examples seem silly, both trivial and vacuous proofs are often used in mathematical induction, as we will see in Chapter 5)]

Proving Conditional Statements: $p \rightarrow q$ 1

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.

(marks the end of the proof. Sometimes **QED** is used instead.)

Proving Conditional Statements: $p \rightarrow q$

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 $\neg q \rightarrow \neg p$ then we have a proof of $p \rightarrow$ q.

Why does this work?

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 $\neg q \rightarrow \neg p$, $p \rightarrow q$ must hold as well. If n is an integer and $3n + 2$ is odd (not even) , then n is odd (not even).

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 $r \wedge \neg r$. (an indirect form of proof). Since we have shown that $\neg p \rightarrow \mathbf{F}$ is true , it follows that the contrapositive $\mathbf{T} \rightarrow p$ 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 of the week, we could only have picked 21 days. This contradicts the assumption that we have picked 22 days.

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 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 $p \leftrightarrow q$.

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

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

Proof Methods and Strategy

Section 1.8

Proof by Cases 1

To prove a conditional statement of the form:

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

Use the tautology

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

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

Proof by Cases 2

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 3

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

$(a \mathbin{@} b) = a$, $a \mathbin{@} c = a$, $b \mathbin{@} c = b$

Hence $(a \mathbin{@} b) \mathbin{@} c = a = a \mathbin{@} (b \mathbin{@} c)$

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.

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)

Nonconstructive Existence Proofs

In a *nonconstructive* existence proof, we 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 √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 $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\sqrt{2})} = \sqrt{2}^{2} = 2$.

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.

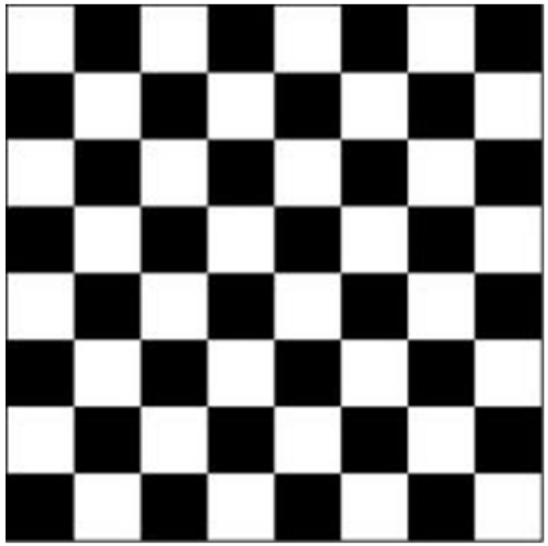
Step n-6: Player$_1$ can leave 12 stones by removing 3 stones.

Now reasoning forward, the first player can ensure a win by removing 3 stones and leaving 12.

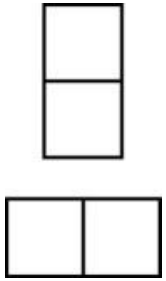
Proof and Disproof: Tilings

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

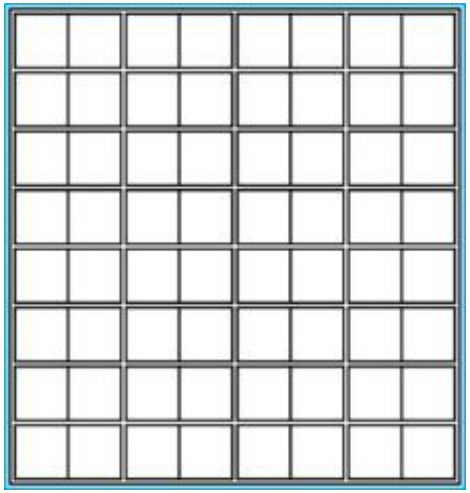
Solution: Yes! One example provides a constructive existence proof



The Standard Checkerboard



Two Dominoes



One Possible Solution

Tilings 1

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.