Discrete Mathematics

Review - Chapter 1, Part III: Proofs

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

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*.

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

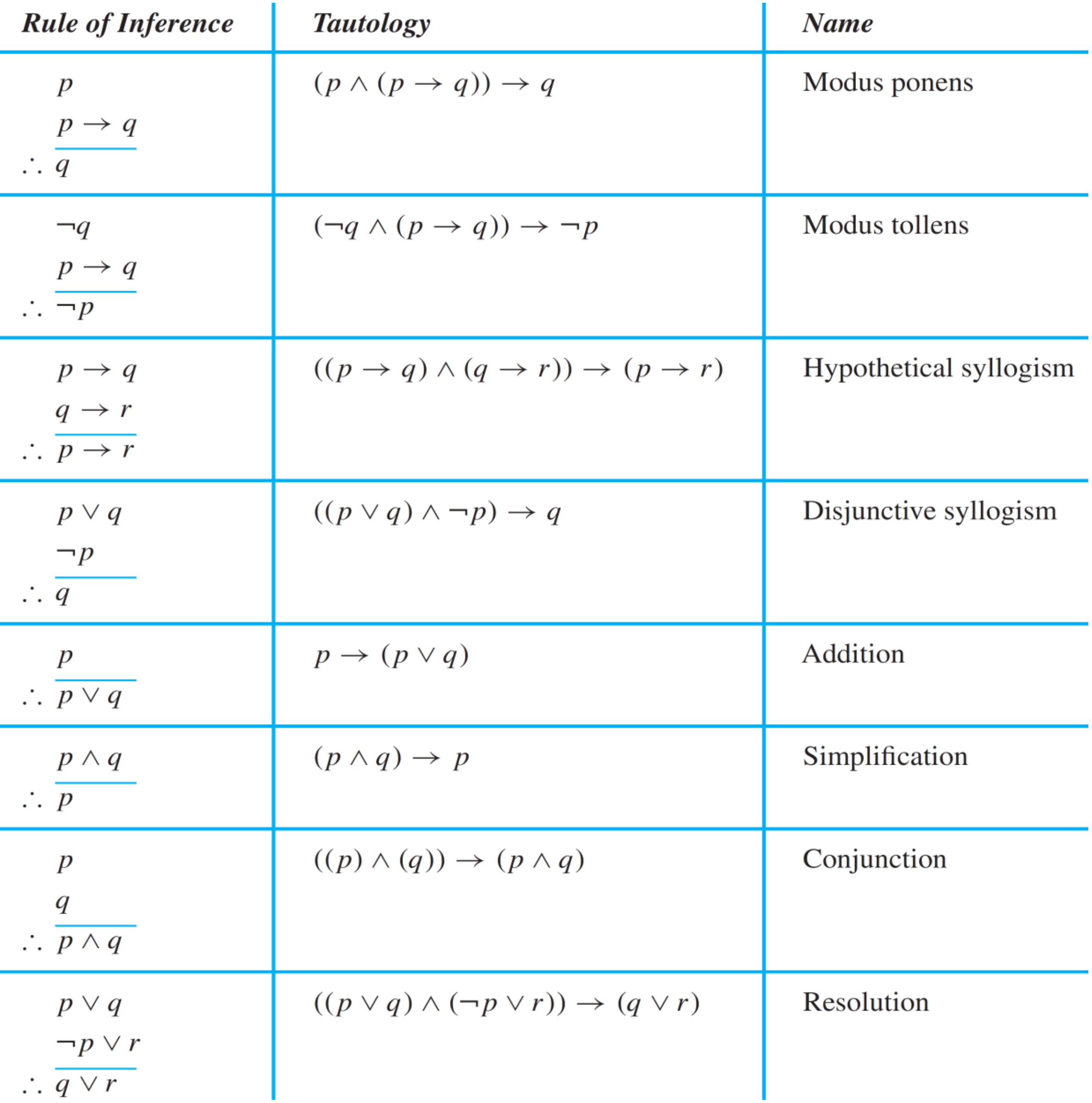
- An *argument form* is an argument that is valid no matter what propositions are substituted into its propositional variables.

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

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

- A *proof* is a valid argument that establishes the truth of a statement.

Rules of inference



Rule of Inference	*Tautology*	*Name*
p $p \to q$ $\therefore q$	$(p \land (p \to q)) \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \land (p \to q)) \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \land (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \lor q$ $\neg p$ $\therefore q$	$((p \lor q) \land \neg p) \to q$	Disjunctive syllogism
p $\therefore p \lor q$	$p \to (p \lor q)$	Addition
$p \land q$ $\therefore p$	$(p \land q) \to p$	Simplification
p q $\therefore p \land q$	$((p) \land (q)) \to (p \land q)$	Conjunction
$p \lor q$ $\neg p \lor r$ $\therefore q \lor r$	$((p \lor q) \land (\neg p \lor r)) \to (q \lor r)$	Resolution

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)

Exercise

Valid Arguments 3

Example 2:

With these hypotheses:

“It is not sunny this afternoon and it is colder than yesterday.”

“If we go swimming then 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:

Step 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.”

Step 2) Translation into propositional logic:

Step 3) Construct the Valid Argument

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

Name	Universal Instantiation (UI)	Universal Generalization (UG)	Existential Instantiation (EI)	Existential Generalization (EG)
Rules of Inference	$\dfrac{\forall x P(x)}{\therefore P(c)}$	$\dfrac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$	$\dfrac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$	$\dfrac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$

- Universal Modus Ponens

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

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

Definitions

- *Proof(증명)* is the explanation of why a statement is true.
- A *theorem(정리)* is a statement that can be shown to be true.
- A *lemma(부명제)* is a '*helping theorem*' or a result which is needed to prove a theorem. (a true statement)
- A *corollary(따름 정리)* is a result which follows directly from a theorem. (a true statement)
- Less important theorems are sometimes called *propositions(명제)*.
- A *conjecture(추측)* 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.

Proving Theorems

Many theorems have the form:

$$\forall x\left(P(x) \rightarrow Q(x)\right)$$

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.

- Ex) "If it is raining then 1=1."

Vacuous Proof: If we know p is false then $p \rightarrow q$ is true as well.

- Ex) "If I am both rich and poor then 2 + 2 = 5."

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

- Ex) "If n is an odd integer, then n^2 is odd."
- Proof) n = 2k+1, and $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2r + 1.$ Thus, n^2 is odd

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.

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.

Proof methods and strategy

- *Proof by Cases*: Prove each statement $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)$ for the original $(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$
- *Constructive existence proof*: Find an x that P(x) is true.
  Example: 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 = $10^3 + 9^3 = 12^3 + 1^3$
  Thus, we found 1729 and $\exists x P(x)$ is true by EG.
- *Nonconstructive Existence Proofs*: Assume no *c* exists which makes *P(c)* true and derive a contradiction. (just check existence)
  Example: 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* = √2 and *y* = √2. But if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x = \sqrt{2}^{\sqrt{2}}$ and *y* = √2 so that $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\,\sqrt{2})} = \sqrt{2}^{2} = 2$ (rational).

Proof methods and strategy

- *Counterexamples*: To establish that $\neg\forall x P(x)$ is true, find a counter example c such that $\neg P(c)$ is True or $P(c)$ is false.

  Example: "Every positive integer is the sum of the squares of 3 integers."
  The integer 7 is a counterexample. So the claim is false.
  Ex) $1 = 1^2+0^2+0^2$ $2 = 1^2+1^2+0^2$ $3 = 1^2+1^2+1^2$ ………….

- *Uniqueness Proofs*: Check Existence and uniqueness for $\exists! x\ P(x)$.
  Existence: an element x with the property exists.
  Uniqueness: 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 $ar + b = 0$.
  Existence: $r = -b/a$ is a solution of $ar + b = 0$
  Uniqueness: Suppose two real numbers (s, r) satisfying $as + b = 0$ and $ar + b = 0$. Then s = r from $ar + b = as + b$.

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.