Chapter 5: Proofs PartA

Discrete Mathematical Structures
MCA 105
Session 2021-22
Odd Semester

Compiled by:
Dr. Sarika Jain
National Institute of Technology Kurukshetra
India
Email: jasarika@nitkkr.ac.in

Most of the slides have been taken from Discrete Mathematics and its Applications, Kenneth H. Rosen, McGraw-Hill Education

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.

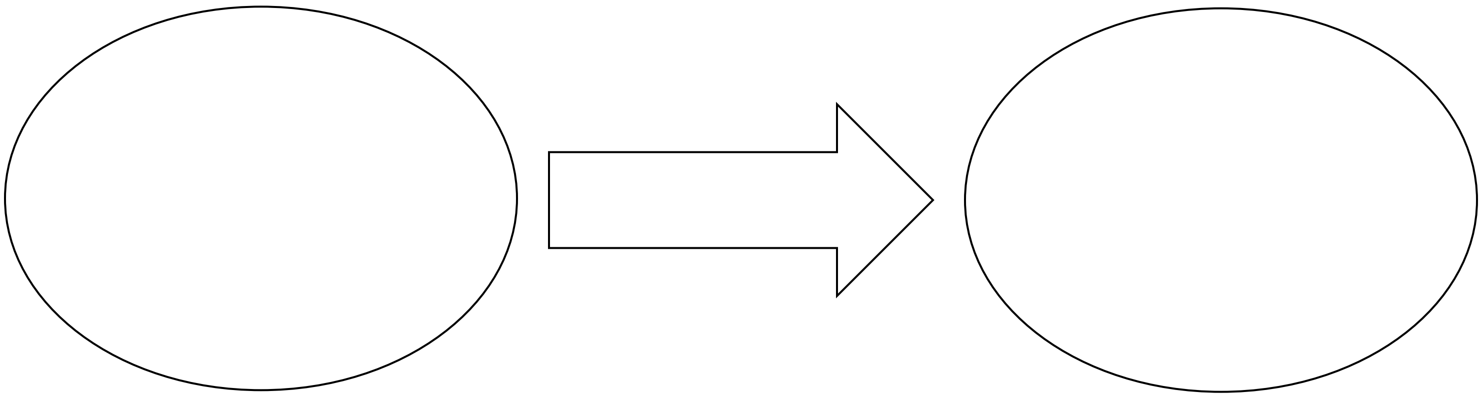
Step n-5: Player$_2$ needs to be faced with 12 stones to be forced to leave 9,10, or 11.

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 in his first move.

Why Proofs?

100s of inputs   input signals ⇒ <u>software</u> ⇒ output signals   > 2^{100s} of possibilities



Software translates input signals to output signals

Proofs can confirm that software works correctly

Testing cannot confirm software correctness

Practice with proofs improves software thinking

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?

Proofs in mathematics are *valid arguments*

An *argument* is a sequence of statements that end in a conclusion

By *valid* we mean the conclusion must follow from the truth of the preceding statements or premises

We use *rules of inference* to construct valid arguments

Valid Arguments in Propositional Logic

Is this a valid argument?

If you listen you will hear what I'm saying
You are listening
Therefore, you hear what I am saying

Let p represent the statement "you listen"
Let q represent the statement "you hear what I am saying"

The argument has the form:

$$\begin{array}{l} p \rightarrow q \\ \underline{p \qquad\quad} \\ \therefore q \end{array}$$

Valid Arguments in Propositional Logic

Argument Form

An argument (in propositional logic) is a sequence of propositions.

All but the final proposition are called ***premises***.

The last proposition is the ***conclusion***

The argument is valid iff the truth of all premises implies the conclusion is true.

An argument form is a sequence of compound propositions.

The argument form with premises $p_1, p_2, \ldots, p_n$

and conclusion q

is valid when $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$ is a tautology

We prove that an argument form is valid by using the laws of inference

Rules of Inference for Propositional Logic: Modus Ponens

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

Corresponding Tautology:

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

Example:

Let p be "Weather is good."

Let q be "I will study discrete math."

"If weather is good, then I will study discrete math."

"Weather is good.

"Therefore , I will study discrete math."

Rules of Inference for Propositional Logic

Rule of inference	Tautology	Name
$p \to q$ p $\therefore q$	$[p \land (p \to q)] \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	$[\neg q \land (p \to q)] \to \neg p$	Modus tollen
$p \to q$ $q \to r$ $\therefore p \to r$	$[(p \to q) \land (q \to r)] \to (p \to r)$	Hypothetic al syllogism
$p \lor q$ $\neg p$ $\therefore q$	$((p \lor q) \land \neg p) \to q$	Disjunctiv e syllogism
p $\therefore p \lor q$	$p \to (p \lor q)$	Addition
$p \land q$ $\therefore p$	$(p \land q) \to p$	Simplifica tion
p q $\therefore p \land q$	$((p) \land (q)) \to (p \land q)$	Conjunctio n
$p \lor q$ $\neg p \lor r$ $\therefore q \lor r$	$[(p \lor q) \land (\neg p \lor r)] \to (p \lor r)$	Resolution

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 "Weather is good.
Let q be "I will study discrete math."

"If weather is good, then I will study discrete math."
"I will not study discrete math."
"Therefore , Weather is not good."

Hypothetical Syllogism

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

Corresponding Tautology:

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

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

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

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 Las Vegas."

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."

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

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

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

Corresponding Tautology:

$$((\neg p \lor r) \land (p \lor q)) \rightarrow (q \lor r)$$

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."

Valid Arguments

Example: 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)

Valid Arguments

Given 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:

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

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)

Fallacies

There are three common mistakes (at least..). These are known as fallacies

1. Fallacy of <u>affirming the conclusion</u> $(q \wedge (p \rightarrow q)) \rightarrow p$

- Affirming the antecedent: Modus ponens $(p \wedge (p \rightarrow q)) \rightarrow q$
- Affirming the conclusion (consequent) is Fallacy $(q \wedge (p \rightarrow q)) \rightarrow p$

2. Fallacy of <u>denying the hypothesis</u> $(\neg p \wedge (p \rightarrow q)) \rightarrow \neg q$

- Denying the consequent: Modus Tollens $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$
- Denying the hypothesis (antecedent) is Fallacy $(\neg p \wedge (p \rightarrow q)) \rightarrow \neg q$

3. Circular reasoning. Here you use the conclusion as an assumption, avoiding an actual proof

    (I know the Bible is true. Bible told me that.)

Problem Example

- For each of these sets of premises, what relevant conclusion or conclusions can be drawn? Explain the rules of inference used to obtain each conclusion from the premises.

  (a) "If I eat spicy foods, then I have strange dreams." "I have strange dreams if there is thunder while I sleep." "I did not have strange dreams."

  (b) "I am dreaming or hallucinating." "I am not dreaming." "If I am hallucinating, I see elephants running down the road."

  (c) "If I work, it is either sunny or partly sunny." "I worked last Monday or I worked last Friday." "It was not sunny on Tuesday." "It was not partly sunny on Friday."

Solution (a)

(a) "If I eat spicy foods, then I have strange dreams." "I have strange dreams if there is thunder while I sleep." "I did not have strange dreams."

- The relevant conclusions are: "I did not eat spicy food" and "There is no thunder while I sleep".
- Let the primitive statements be:
  - *s, 'I eat spicy foods'*
  - *d, 'I have strange dreams'*
  - *t, 'There is thunder while I sleep'*
- Then the premises are translated as: $s \to d$, $t \to d$, and $\neg d$.
- And the conclusions: $\neg s$, $\neg t$.

Steps		Reason
1.	$s \to d$	*premise*
2.	$\neg d$	*premise*
3.	$\neg s$	*Modus Tollens to Steps 1 and 2*
4.	$t \to d$	*premise*
5.	$\neg t$	*Modus Tollens to Steps 4 and 2.*

Solution (b)

(b) "I am dreaming or hallucinating." "I am not dreaming." "If I am hallucinating, I see elephants running down the road."

- The relevant conclusion is: "I see elephants running down the road."
- Let the primitive statements be:
  - *d, 'I am dreaming'*
  - *h, 'I am hallucinating'*
  - *e, 'I see elephants running down the road'*
- Then the premises are translated as: $d \lor h$, $\neg d$, and $h \rightarrow e$.
- And the conclusion: e.

Steps	**Reason**
1. $d \lor h$	*premise*
2. $\neg d$	*premise*
3. h	*rule of disjunctive syllogism to Steps 1 and 2*
4. $h \rightarrow e$	*premise*
5. e	*Modus Ponens to Steps 4 and 3*

Solution (c)

(c) "If I work, it is either sunny or partly sunny." "I worked last Monday or I worked last Friday." "It was not sunny on Tuesday." "It was not partly sunny on Friday."

- There is no single relevant conclusion in this problem, its main difficulty is to to represent the premises so that one is able infer anything at all. One possible relevant conclusion is: "It was sunny or partly sunny last Monday or it was sunny last Friday.".
- Let the primitive statements be:
  - *wm, 'I worked last Monday'*
  - *wf , 'I worked last Friday'*
  - *sm, 'It was sunny last Monday'*
  - *st, 'It was sunny last Tuesday'*
  - *sf , 'It was sunny last Friday'*
  - *pm, 'It was partly sunny last Monday'*
  - *pf , 'It was partly sunny last Friday'*
- Then the premises are translated as: $wm \lor wf$, $wm \rightarrow (sm \lor pm)$, $wf \rightarrow (sf \lor pf)$, $\neg st$, and $\neg pf$.
- And the conclusion: $sf \lor sm \lor pm$.

Solution (c) – Method 1

Steps		Reason
1.	$wf \rightarrow (sf \lor pf)$	*premise*
2.	$\neg wf \lor sf \lor pf$	*expression for implication*
3.	$\neg pf \rightarrow (\neg wf \lor sf)$	*expression for implication*
4.	$\neg pf$	*premise*
5.	$\neg wf \lor sf$	*modus ponens to Steps 3 and 4*
6.	$wf \rightarrow sf$	*expression for implication*
7.	$wm \lor wf$	*premise*
8.	$\neg wm \rightarrow wf$	*expression for implication*
9.	$\neg wm \rightarrow sf$	*rule of syllogism to Steps 8 and 6*
10.	$wm \lor sf$	*expression for implication*
11.	$\neg sf \rightarrow wm$	*expression for implication*
12.	$wm \rightarrow (sm \lor pm)$	*premise*
13.	$\neg sf \rightarrow (sm \lor pm)$	*rule of syllogism to Steps 11 and 12*
14.	$sf \lor sm \lor pm$	*expression for implication.*

Solution (c) – Method 2 (Use resolution)

Steps	Reason
1. $wf \rightarrow (sf \lor pf)$	*premise*
2. $\neg wf \lor sf \lor pf$	*expression for implication*
3. $\neg pf$	*premise*
4. $\neg wf \lor sf$	*rule of resolution to Steps 2 and 3*
5. $wm \lor wf$	*premise*
6. $wm \lor sf$	*rule of resolution to Steps 4 and 5*
7. $wm \rightarrow (sm \lor pm)$	*premise*
8. $\neg wm \lor sm \lor pm$	*expression for implication*
9. $sf \lor sm \lor pm$	*rule of resolution to Steps 7 and 8*

Rule of Inference for Predicate Logic

- Inference rules for propositional logic apply to predicate logic as well
  - Modus Ponens, Modus tollens etc.
- New (sound) inference rules for use with quantifiers:
  - Universal Instantiation
  - Existential Instantiation
  - Existential Generalization
  - Universal Modus Ponens

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.”

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."

This is inverse of Existential Instantiation

Another Example:
Eats(Ziggy, IceCream)
$\exists$ x Eats(Ziggy, x)

Valid Argument using UI

Example: 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 $M(x)$: "x is a man"

$L(x)$: "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)

Valid Argument using UI, EI, and EG

Example: 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 $C(x)$: "x is in this class,"

$B(x)$: "x has read the book,"

$P(x)$: "x passed the first exam."

First we translate the premises and conclusion into symbolic form.

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

Valid Argument using UI, EI, and EG

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. $\forall x(C(x) \to P(x))$	Premise
5. $C(a) \to P(a)$	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

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

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

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 (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.

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

This rule could be used in the Socrates example.

Example

- Given the hypotheses:
  - "If it does not rain or if it is not foggy, then the sailing race will be held and the lifesaving demonstration will go on"
  - "If the sailing race is held, then the trophy will be awarded"
  - "The trophy was not awarded"
- Can you conclude: "It rained"?

$(\neg r \lor \neg f) \rightarrow (s \land l)$

$s \rightarrow t$

$\neg t$

---

r

Example

1. $\neg t$ — 3rd hypothesis
2. $s \rightarrow t$ — 2nd hypothesis
3. $\neg s$ — Modus tollens using steps 2 & 3
4. $(\neg r \vee \neg f) \rightarrow (s \wedge l)$ — 1st hypothesis
5. $\neg(s \wedge l) \rightarrow \neg(\neg r \vee \neg f)$ — Contrapositive of step 4
6. $(\neg s \vee \neg l) \rightarrow (r \wedge f)$ — DeMorgan's law and double negation law
7. $\neg s \vee \neg l$ — Addition from step 3
8. $r \wedge f$ — Modus ponens using steps 6 & 7
9. r — Simplification using step 8

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

Example

- Show that "A car in the garage has an engine problem" and "Every car in the garage has been sold" imply the conclusion "A car that has been sold has an engine problem"
- Let
  - $G(x)$: "x is in the garage"
  - $E(x)$: "x has an engine problem"
  - $S(x)$: "x has been sold"
- Let UoD be the set of all cars
- The premises are as follows:
  - $\exists x\, (G(x) \land E(x))$
  - $\forall x\, (G(x) \rightarrow S(x))$
- The conclusion we want to show is: $\exists x\, (S(x) \land E(x))$

Solution

1. $\exists x\,(G(x) \land E(x))$ *1st premise*
2. $(G(c) \land E(c))$ *Existential instantiation of (1)*
3. $G(c)$ *Simplification of (2)*
4. $\forall x\,(G(x) \rightarrow S(x))$ *2nd premise*
5. $G(c) \rightarrow S(c)$ *Universal instantiation of (4)*
6. $S(c)$ *Modus ponens on (3) and (5)*
7. $E(c)$ *Simplification from (2)*
8. $S(c) \land E(c)$ *Conjunction of (6) and (7)*
9. $\exists x\,(S(x) \land E(x))$ *Existential generalization of (8)*

PRACTICE

- Consider the following english text:

  “Anyone passing his Intelligent System exam and winning the lottery is happy. But any student who studies for an exam or is lucky can pass all his exams. John did not study but John is lucky. Anyone who is lucky wins the lottery. Mary did not win the lottery, however Mary passed her IS exam. Gary won the lottery. Gary, John, and Mary are all students.“

- Is John happy?
- Is Mary happy? Is she lucky?
- Did every student pass the IS exam?

Formalization in FOL

1. Encode general knowledge of the domain

- Anyone passing the IS exams and winning the lottery is happy
  $\forall x\ Pass(x, IS) \land Win(x, Lottery) \Rightarrow Happy(x)$
- Any student who studies or is lucky can pass all his exams
  $\forall x\ \forall y\ Student(x) \land Exam(y) \land (StudiesFor(x, y) \lor Lucky(x)) \Rightarrow Pass(x,y)$
- Anyone who is lucky wins the lottery
  $\forall x\ Lucky(x) \Rightarrow Win(x, Lottery)$

Formalization in FOL

2. Encode the specific problem instance

- John did not study, but John is lucky
  $\neg Study(John) \wedge Lucky(John)$
- Mary did not win the lottery, however Mary passed her IS exam
  $\neg$ Win(Mary, Lottery)
  Pass(Mary,IS)
- Gary won the lottery
  Win(Gary, Lottery)
- Gary, John, and Mary are all students
  Student(Gary), Student(John), Student(Mary)

Formalization in FOL

3. Pose queries to the inference procedure

- Is John happy?

  Happy(John) ?

- Is Mary happy? Is she lucky?

  Happy(Mary), Lucky(Mary)?

- Did every student pass the IS exam?

  $\exists$ x Student(x) $\wedge$ Pass(x, IS) ?

Resources

1. Discrete Mathematics and its Applications, Kenneth H. Rosen
2. https://www.people.vcu.edu/~rhammack/BookOfProof/
3. My ppt slides
4. Google