CSE2023 Discrete Computational Structures

Lecture 4

Methods of Proof

- When is a mathematical argument correct?
- What methods can be used to construct mathematical arguments?
- Important in many computer science applications
  - Verify a computer program is correct
  - To establish a OS is secure
  - Making inferences n AI
  - Show system specs are consistent
  - ...

1.6 Rules of Inference

- **Proof**: valid arguments that establish the truth of a mathematical statement
- **Argument**: a sequence of statements that end with a conclusion
- **Valid**: the conclusion or final statement of the argument must follow the truth of proceeding statements or **premise** of the argument

Argument and inference

- An **argument** is valid *if and only if* it is *impossible* for all the premises to be *true* and the conclusion to be *false*
- Rules of **inference**: use them to deduce (construct) new statements from statements that we already have
- Basic tools for establishing the truth of statements

Valid arguments in propositional logic

- Consider the following arguments involving propositions

"If you have a correct password, then you can log onto the network"

"You have a correct password"

premises

therefore,

"You can log onto the network"

conclusion

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

Valid arguments

- $((p \to q) \land p) \to q$ is tautology
- When ((p→q)^p) is true, both p→q and p are true, and thus q must be also be true
- This form of argument is true because when the premises are true, the conclusion must be true

Example

- p: "You have access to the network"
- q: "You can change your grade"
- p→q: "If you have access to the network, then you can change your grade"

"If you have access to the network, then you can change your grade" (p→q)

"You have access to the network" (p)

so "You can change your grade" (q)

Example

"If you have access to the network, then you can change your grade" (p→q)

"You have access to the network" (p)

so "You can change your grade" (q)

- Valid arguments
- But the conclusion is not true
- **Argument form**: a sequence of compound propositions involving propositional variables

Rules of inference for propositional logic

- Can always use truth table to show an argument form is valid
- For an argument form with 10 propositional variables, the truth table requires 2^{10} rows
- The tautology $((p \to q) \wedge p) \to q$ is the rule of inference called **modus ponens** (*mode that affirms*), or the **law of detachment**

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

Example

- If both statements "If it snows today, then we will go skiing" and "It is snowing today" are true.
- By modus ponens, it follows the conclusion "We will go skiing" is true

Example

If $\sqrt{2} > \frac{3}{2}$ then $(\sqrt{2})^2 > (\frac{3}{2})^2$. We know that $\sqrt{2} > \frac{3}{2}$

Consequently, $(\sqrt{2})^2 = 2 > (\frac{3}{2})^2 = \frac{9}{4}$

Is it a valid argument? Is conclusion true?

- The premises of the argument are p→q and p, and q is the conclusion
- This argument is valid by using modus ponens
- But one of the premises is false, consequently we cannot conclude the conclusion is true
- Furthermore, the conclusion is not true

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
$\begin{array}{l} \quad p \\ \quad p \to q \\ \hline \therefore q \end{array}$	$[p \wedge (p \to q)] \to q$	Modus ponens
$\begin{array}{l} \quad \neg q \\ \quad p \to q \\ \hline \therefore \neg p \end{array}$	$[\neg q \wedge (p \to q)] \to \neg p$	Modus tollens
$\begin{array}{l} \quad p \to q \\ \quad q \to r \\ \hline \therefore p \to r \end{array}$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$	Hypothetical syllogism
$\begin{array}{l} \quad p \vee q \\ \quad \neg p \\ \hline \therefore q \end{array}$	$[(p \vee q) \wedge \neg p] \to q$	Disjunctive syllogism

p $\therefore \overline{p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$p \wedge q$ $\therefore \overline{p}$	$(p \wedge q) \rightarrow p$	Simplification
p q $\therefore \overline{p \wedge q}$	$[(p) \wedge (q)] \rightarrow (p \wedge q)$	Conjunction
$p \vee q$ $\neg p \vee r$ $\therefore \overline{q \vee r}$	$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$	Resolution

Example

- "It is not sunny this afternoon and it is colder than yesterday" $\neg p \wedge q$
- "We will go swimming only if it is sunny" $r \rightarrow p$
- "If we do not go swimming, then we will take a canoe trip" $\neg r \rightarrow s$
- "If we take a canoe trip, then we will be home by sunset" $s \rightarrow t$

1) $\neg p \wedge q$	hypothesis
2) $\neg p$	simplication using (1)
3) $r \rightarrow p$	hypothesis
4) $\neg r$	modus tollens using (2) and (3)
5) $\neg r \rightarrow s$	hypothesis
6) s	modus ponens using (4)
7) $s \rightarrow t$	hypothesis
8) t	modus ponens using (6) and (7)

Can we conclude t

"We will be home by sunset"?

Example

- "If you send me an email message, then I will finish my program" $p \rightarrow q$
- "If you do not send me an email message, then I will go to sleep early" $\neg p \rightarrow r$
- "If I go to sleep early, then I will wake up feeling refreshed" $r \rightarrow s$

1) $p \rightarrow q$	hypothesis
2) $\neg q \rightarrow \neg p$	contrapositive of (1)
3) $\neg p \rightarrow r$	hypothesis
4) $\neg q \rightarrow r$	hypothetical syllogism using (2) and (3)
5) $r \rightarrow s$	hypothesis
6) $\neg q \rightarrow s$	hypothetical syllogism using (4) and (5)

- "If I do not finish writing the program, then I will wake up feeling refreshed" $\neg q \rightarrow s$

Resolution

- Based on the tautology $((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$
- Resolvent: $q \vee r$
- Let q=r, we have $(p \vee q) \wedge (\neg p \vee q) \rightarrow q$
- Let r=F, we have $(p \vee q) \wedge \neg p \rightarrow q$
- Important in logic programming, AI, etc.

Example

- "Jasmine is skiing or it is not snowing" $q \vee \neg p$
- "It is snowing or Bart is playing hockey" $p \vee r$

imply $q \vee r$

- "Jasmine is skiing or Bart is playing hockey"

17

Example

- To construct proofs using resolution as the only rule of inference, the hypotheses and the conclusion must be expressed as clauses
- **Clause**: a disjunction of variables or negations of these variables

Show $(p \wedge q) \vee r$ and $r \rightarrow s$ imply $p \vee s$

$(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$

$r \rightarrow s \equiv \neg r \vee s$

18

Fallacies

- Inaccurate arguments
- $((p \rightarrow q) \wedge q) \rightarrow p$ is not a tautology as it is false when p is false and q is true
- If you do every problem in this book, then you will learn discrete mathematics. You learned discrete mathematics

Therefore you did every problem in this book

$(p \rightarrow q) \wedge q$

19

Inference with quantified statements

TABLE 2 Rules of Inference for Quantified Statements.

Rule of Inference	*Name*
$\forall x P(x)$ / $\therefore P(c)$	Universal instantiation
$P(c)$ for an arbitrary c / $\therefore \forall x P(x)$	Universal generalization
$\exists x P(x)$ / $\therefore P(c)$ for some element c	Existential instantiation
$P(c)$ for some element c / $\therefore \exists x P(x)$	Existential generalization

Instantiation:
c is one *particular* member of the domain

Generalization:
for an *arbitrary* member c

21

Example

- "Everyone in this discrete mathematics has taken a course in computer science" and "Marla is a student in this class" imply "Marla has taken a course in computer science"

$1. \forall x(d(x) \rightarrow c(x))$	premise
$2. d(Marla) \rightarrow c(Marla)$	universal instantiation from (1)
$3. d(Marla)$	premise
$4. c(Marla)$	modus ponens from (2) and (3)

Example

- "A student in this class has not read the book", and "Everyone in this class passed the first exam" imply "Someone who passed the first exam has not read the book"

$1. \exists x(c(x) \wedge \neg b(x))$	premise
$2. c(a) \wedge \neg b(a)$	existential instantiation from (1)
$3. c(a)$	simpliciation from (2)
$4. \forall x(c(x) \rightarrow p(x)$	premise
$5. c(a) \rightarrow p(a)$	universal instantiation from (4)
$6. p(a)$	modus ponens from (3) and (5)
$7. \neg b(a)$	simplication from (2)
$8. p(a) \wedge \neg b(a)$	conjunction of (6) and (7)
$9. \exists x(p(x) \wedge \neg b(x))$	existential generalization form (8)

Universal modus ponens

- Use universal instantiation and modus ponens to derive new rule

$$\begin{array}{l} \forall x(p(x) \rightarrow q(x)) \\ \underline{p(a), \text{ where a is a particular element in the domain}} \\ \therefore q(a) \end{array}$$

- Assume "For all positive integers n, if n is greater than 4, then n^2 is less than 2^n" is true. Show $100^2<2^{100}$

Universal modus tollens

- Combine universal modus tollens and universal instantiation

$$\begin{array}{l} \forall x(p(x) \rightarrow q(x)) \\ \underline{\neg q(a), \text{ where a is a particular element in the domain}} \\ \therefore \neg p(a) \end{array}$$