CPSC 121: Models of Computation

Unit 4

Propositional Logic Proofs

Based on slides by Patrice Belleville and Steve Wolfman

Pre-Class Learning Goals

- By the start of this class you should be able to
  - Use truth tables to establish or refute the validity of a rule of inference.
  - Given a rule of inference and propositional logic statements that correspond to the rule's premises, apply the rule to infer a new statement implied by the original statements.

Quiz 4 Feedback:

- Overall:
- Issues:
- We will discuss the open-ended question soon.

In-Class Learning Goals

- By the end of this unit, you should be able to
  - Determine whether or not a propositional logic proof is valid, and explain why it is valid or invalid.
  - Explore the consequences of a set of propositional logic statements by application of equivalence and inference rules, especially in order to massage statements into a desired form.
  - Devise and attempt multiple different, appropriate strategies for proving a propositional logic statement follows from a list or premises.

Where We Are in The Big Stories

- Theory:
  - How can we convince ourselves that an algorithm does what it's supposed to do?
- In general
  - We need to prove that it works.
- We have done a few proofs last week.
- Now we will learn
  - How to decide if a proof is valid in a formal setting.
  - How to write proofs in English.

What is Proof?

- A rigorous formal argument that demonstrates the truth of a proposition, given the truth of the proof's premises.
- In other words:
  - A proof is used to convince other people (or yourself) of the truth of a conditional proposition.
  - Every step must be well justified.
- Writing a proof is a bit like writing a function:
  - you do it step by step, and
  - make sure that you understand how each step relates to the previous steps.

Things we'd like to prove

- We can build a combinational circuit matching any truth table.
- We can build any digital logic circuit using only 2-input NAND gates.
- The maximum number of swaps we need to order n students is $n(n-1)/2$.
- No general algorithm exists to sort n values using fewer than $n \log_2 n$ comparisons.
- There are problems that no algorithm can solve.

What is a Propositional Logic Proof

- A propositional logic proof consists of a sequence of propositions, where each proposition is one of
  - a premise
  - the result of applying a logical equivalence or a **rule of inference** to one or more earlier propositions.

  and whose last proposition is the conclusion.
- These are good starting point, because they are simpler than the more free-form proofs we will discuss later
  - Only a limited number of choices at each step.

Meaning of Proof

- Suppose you proved this:

  Premise-1
  Premise-2
  ...
  Premise-n

  ∴Conclusion

- What does it mean?

  A. Premises 1 to n may be true
  B. Premises 1 to n are true
  C. Conclusion may be true
  D. Conclusion is true
  E. None of the above.

Meaning of Proof

- What does this argument mean?

  Premise-1
  Premise-2
  ...
  Premise-n

  ∴Conclusion

  A. Premise-1 ∧ … ∧ Premise-n ∧ Conclusion
  B. Premise-1 ∨ … ∨ Premise-n ∨ Conclusion
  C. Premise-1 ∧ … ∧ Premise-n → Conclusion
  D. Premise-1 ∧ … ∧ Premise-n ↔ Conclusion
  E. None of the above.

Why do we want valid rules?

Consider…

p
q → p
∴ q

Can q be false when p and q → p are both true?

a. Yes
b. No
c. Not enough information
d. I don't know

Why do we want valid rules?

"Degenerate" cases:

p ∧ ~p
∴ I_got_110%_in_121

Can **I_got_110%_in_121** be false when (p ∧ ~p) is true?

a. Yes
b. No
c. Not enough information
d. I don't know

Why do we want valid rules?

~p

∴ **~(p v q)**

a. This is *valid* by generalization (p ⇒ p v q).
b. This is *valid* because anytime ~p is true, ~(p v q) is also true.
c. This is *valid* by some other rule.
d. This is *invalid* because when p = F and q = T, ~p is true but ~(p v q) is false.
e. None of these.

Basic Rules of Inference

Modus Ponens: [M.PON] **p → q, p / q**	Modus Tollens: [M.TOL] **p → q, ~q / ~p**
Generalization: [GEN] **p / p v q** ; **p / q → p**	Specialization: [SPEC] **p ∧ q / p** ; **p ∧ q / q**
Conjunction: [CONJ] **p, q / p ∧ q**	Elimination: [ELIM] **p v q, ~p / q** ; **p v q, ~q / p**
Transitivity: [TRANS] **p → q, q → r / p → r**	Proof by cases: [CASE] **p v q, p → r, q → r / r**
Contradiction: [CONT] **p → F / ~p**	

Onnagata Problem from Online Quiz #4

- Critique the following argument, drawn from an article by Julian Baggini on logical fallacies.
  - **Premise 1**: If women are too close to femininity to portray women then men must be too close to masculinity to play men, and vice versa.
  - **Premise 2**: And yet, if the onnagata are correct, women are too close to femininity to portray women and yet men are not too close to masculinity to play men.
  - **Conclusion**: Therefore, the onnagata are incorrect, and women are not too close to femininity to portray women.
- Note: onnagata are male actors portraying female characters in kabuki theatre.

Onnagata Problem

Which definitions should we use?

a) w = women, m = men, f = femininity, m = masculinity, o = onnagata, c = correct
b) w = women are too close to femininity, m = men are too close to masculinity, pw = women portray women, pm = men portray men, o = onnagata are correct
c) w = women are too close to femininity to portray women, m = men are too close to masculinity to portray men, o = onnagata are correct
d) None of these, but another set of definitions works well.
e) None of these, and this problem cannot be modeled well with propositional logic.

Onnagata Problem

- Which of these is *not* an accurate translation of one of the statements?
  A. $w \leftrightarrow m$
  B. $(w \rightarrow m) \wedge (m \rightarrow w)$
  C. $o \rightarrow (w \wedge \sim m)$
  D. $\sim o \wedge \sim w$
  E. All of these are accurate translations.
- So, the argument is:

Onnagata Problem

- Do the two premises contradict each other (that is, is $p1 \wedge p2 \equiv F$)?
  A. Yes
  B. No
  C. Not enough information to tell
- Is the argument valid?
  - A: Yes
  - B: No
  - C: ?

Onnagata Problem

- What can we prove?
- Can we prove that the Onnagata are wrong.
  A. Yes
  B. No
  C. Not enough information
- Can we prove that women are not too close to femininity to portray women?
  A. Yes
  B. No
  C. Not enough information
- What other scenario is consistent with the premises?

Proof Strategies

- Look at the information you have
  - Is there irrelevant information you can ignore?
  - Is there critical information you should focus on?
- Work backwards from the end
  - Especially if you have made some progress but are missing a step or two.
- Don't be afraid of inferring new propositions, even if you are not quite sure whether or not they will help you get to the conclusion you want.

Proof strategies (continued)

- If you are not sure of the conclusion, alternate between
  - trying to find an example that shows the statement is false, using the place where your proof failed to help you design the counterexample
  - trying to prove it, using your failed counterexample to help you write the proof.

Example

- To prove:

  $\sim(q \vee r)$

  $(u \wedge q) \leftrightarrow s$

  $\sim s \rightarrow \sim p$

  $\therefore \sim p$

- What will the strategy be?
  - A. Derive $\sim u$ so you can derive $\sim s$
  - B. Derive $u \wedge q$ so you can get s
  - C. Derive $\sim s$ by deriving first $\sim(u \wedge q)$
  - D. Any of the above will work
  - E. None of the above will work

Example (cont')

$\sim(q \vee r)$
$(u \wedge q) \leftrightarrow s$
$\sim s \rightarrow \sim p$
$\therefore \sim p$

Proof:

1. $\sim(q \vee r)$	Premise
2. $(u \wedge q) \leftrightarrow s$	Premise
3. $\sim s \rightarrow \sim p$	Premise
4. $\sim q \wedge \sim r$	De Morgan's (1)
5. $\sim q$	Specialization (4)
6. $((u \wedge q) \rightarrow s) \wedge (s \rightarrow (u \wedge q))$	Bicond (2)
7. $s \rightarrow (u \wedge q)$	Specialization (6)
8. ????	????
9. $\sim(u \wedge q)$	????
10. $\sim s$	Modus tollens (7, 9)
11. $\sim p$	Modus ponens (3,10)

- What is in step 8?
  - A. $u \wedge q$
  - B. $\sim u \vee \sim q$
  - C. s
  - D. $\sim s$
  - E. None of the above

Example (cont')

$\sim(q \vee r)$
$(u \wedge q) \leftrightarrow s$
$\sim s \rightarrow \sim p$
$\therefore \sim p$

Proof:

1. $\sim(q \vee r)$	Premise
2. $(u \wedge q) \leftrightarrow s$	Premise
3. $\sim s \rightarrow \sim p$	Premise
4. $\sim q \wedge \sim r$	De Morgan's (1)
5. $\sim q$	Specialization (4)
6. $((u \wedge q) \rightarrow s) \wedge (s \rightarrow (u \wedge q))$	Bicond (2)
7. $s \rightarrow (u \wedge q)$	Specialization (6)
8. ????	????
9. $\sim(u \wedge q)$	????
10. $\sim s$	Modus tollens (7, 9)
11. $\sim p$	Modus ponens (3,10)

- Which rule was used in step 8?
  - A. modus ponens
  - B. De Morgan's
  - C. modus tollens
  - D. generalization
  - E. None of the above

Example (cont')

$\neg(q \vee r)$
$(u \wedge q) \leftrightarrow s$
$\neg s \rightarrow \neg p$
$\therefore \neg p$

Proof:

1. $\neg(q \vee r)$	Premise
2. $(u \wedge q) \leftrightarrow s$	Premise
3. $\neg s \rightarrow \neg p$	Premise
4. $\neg q \wedge \neg r$	De Morgan's (1)
5. $\neg q$	Specialization (4)
6. $((u \wedge q) \rightarrow s) \wedge (s \rightarrow (u \wedge q))$	Bicond (2)
7. $s \rightarrow (u \wedge q)$	Specialization (6)
8. ????	????
9. $\neg(u \wedge q)$	????
10. $\neg s$	Modus tollens (7, 9)
11. $\neg p$	Modus ponens (3,10)

- Which rule was used in step 9?
  - A. modus ponens
  - B. De Morgan's
  - C. modus tollens
  - D. generalization
  - E. None of the above

Another Example

- Prove the following argument:

p
$p \rightarrow r$
$p \rightarrow (q \vee \neg r)$
$\neg q \vee \neg s$
$\therefore s$

Limitations of Truth Tables

- Why can we not just use truth tables to prove propositional logic theorems?
  - A. No reason; truth tables are enough.
  - B. Truth tables scale poorly to large problems.
  - C. Rules of inference and equivalence rules can prove theorems that cannot be proven with truth tables.
  - D. Truth tables require insight to use, while rules of inference can be applied mechanically.

Limitations of Logical Equivalences

- Why not use logical equivalences to prove that the conclusions follow from the premises?
  - A. No reason; logical equivalences are enough.
  - B. Logical equivalences scale poorly to large problems.
  - C. Rules of inference and truth tables can prove theorems that cannot be proven with logical equivalences.
  - D. Logical equivalences require insight to use, while rules of inference can be applied mechanically.

One More Remark

- Consider the following:

  George is rich

  If George is rich then he will pay your tuition

  ∴ George will pay your tuition.

- Is this argument valid?
  - A. Yes
  - B. No
  - C. Not enough information to tell
- Should you pay your tuition, or should you assume that George will pay it for you? Why?

Exercises

- Prove that the following argument is valid:

  $p \rightarrow q$

  $q \rightarrow (r \wedge s)$

  $\neg r \vee (\neg t \vee u)$

  $p \wedge t$

  ∴ u

- Given the following premises, what can you prove?

  $p \rightarrow q$

  $p \vee \neg q \vee r$

  $(r \wedge \neg p) \vee s \vee \neg p$

  $\neg r$

Further Exercises

- Hercule Poirot has been asked by Lord Maabo to find out who closed the lid of his piano after dumping the cat inside. Poirot interrogates two of the servants, Akilna and Eiluj. One and only one of them put the cat in the piano. Plus, one always lies and one never lies.
  - Eiluj: I did not put the cat in the piano. Urquhart gave me less than $60 to help him study.
  - Akilna: Eiluj did it. Urquhart paid her $50 to help him study.
- Who put the cat in the piano?

Reading for Next Lecture

- Online quiz #5 is tentatively due _____
- Assigned reading for the quiz:
  - Epp, 4th edition: 3.1, 3.3
  - Epp, 3rd edition: 2.1, 2.3
  - Rosen, 6th edition: 1.3, 1.4
  - Rosen, 7th edition: 1.4, 1.5