

Proof Methods

22c:19, Chapter 3
Hantao Zhang

1

Proof methods

- We will discuss ten proof methods:
 1. Direct proofs
 2. Indirect proofs
 3. Vacuous proofs
 4. Trivial proofs
 5. Proof by contradiction
 6. Proof by cases
 7. Proofs of equivalence
 8. Existence proofs
 9. Uniqueness proofs
 10. Counterexamples

2

Direct proofs

- Consider an implication: $p \rightarrow q$
 - If p is false, then the implication is always true
 - Thus, show that if p is true, then q is true
- To perform a direct proof, assume that p is true, and show that q must therefore be true

3

Direct proof example

- Show that the square of an even number is an even number
- Rephrased: if n is even, then n^2 is even
- Assume n is even
 - Thus, $n = 2k$, for some k (definition of even numbers)
 - $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$
 - As n^2 is 2 times an integer, n^2 is thus even

4

Indirect proofs

- Consider an implication: $p \rightarrow q$
 - It's contrapositive is $\neg q \rightarrow \neg p$
 - Is logically equivalent to the original implication!
 - Thus, show that if $\neg q$ is true, then $\neg p$ is true
- To perform an indirect proof, do a direct proof on the contrapositive

5

Indirect proof example

- If n^2 is an odd integer then n is an odd integer
- Prove the contrapositive: If n is an even integer, then n^2 is an even integer
- Proof: $n=2k$ for some integer k (definition of even numbers)
- $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$
- Since n^2 is 2 times an integer, it is even

6

Which to use

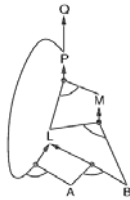
- When do you use a direct proof versus an indirect proof?
- If it's not clear from the problem, try direct first, then indirect second
 - If indirect fails, try other proof methods

7

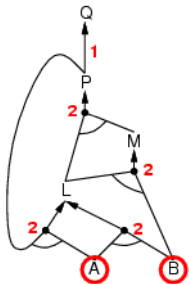
Direct Proof: Forward chaining

- Idea: fire any rule whose premises are known to be true
 - Remember its conclusion as true, until what you wanted is found
 - Example: Is Q true?

$P \Rightarrow Q$
 $L \wedge M \Rightarrow P$
 $B \wedge L \Rightarrow M$
 $A \wedge P \Rightarrow L$
 $A \wedge B \Rightarrow L$
 A
 B

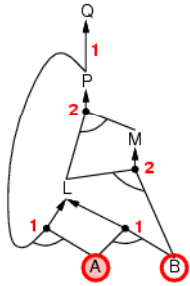


Forward chaining example



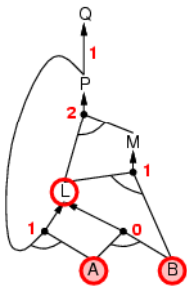
$P \Rightarrow Q$
 $L \wedge M \Rightarrow P$
 $B \wedge L \Rightarrow M$
 $A \wedge P \Rightarrow L$
 $A \wedge B \Rightarrow L$
 A
 B

Forward chaining example



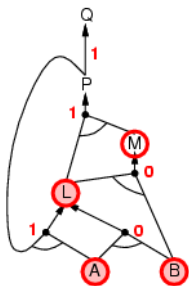
- $P \Rightarrow Q$
- $L \wedge M \Rightarrow P$
- $B \wedge L \Rightarrow M$
- $A \wedge P \Rightarrow L$
- $A \wedge B \Rightarrow L$
- A
- B

Forward chaining example

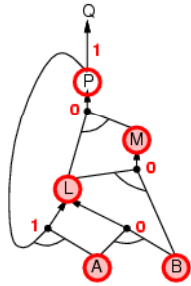


- $P \Rightarrow Q$
- $L \wedge M \Rightarrow P$
- $B \wedge L \Rightarrow M$
- $A \wedge P \Rightarrow L$
- $A \wedge B \Rightarrow L$
- A
- B

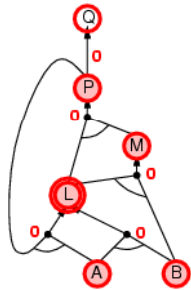
Forward chaining example



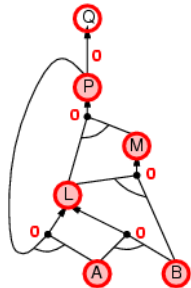
Forward chaining example



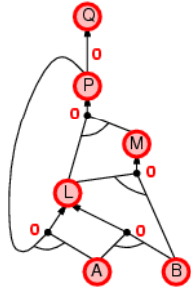
Forward chaining example



Forward chaining example



Forward chaining example



Indirect Proof: Backward chaining

Idea: Work backwards from what you wanted to know.

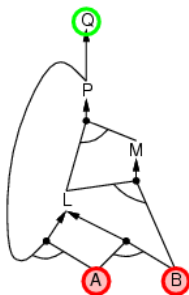
The goal is q , i.e., prove that q is true:

1. Check if q is already known to be true (goal is found), or
2. Prove by Backward chaining that all premises of some rule concluding q are true (goal reduction). That is, we know

$$a \wedge b \wedge c \rightarrow q$$

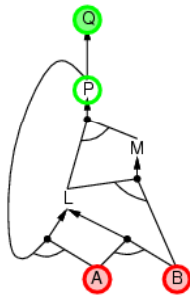
and we want to prove that a, b, c (called subgoals) are all true by the same approach.

Backward chaining example



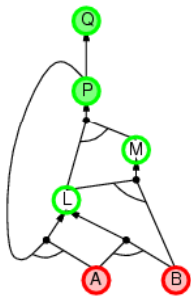
- $P \Rightarrow Q$
- $L \wedge M \Rightarrow P$
- $B \wedge L \Rightarrow M$
- $A \wedge P \Rightarrow L$
- $A \wedge B \Rightarrow L$
- A
- B

Backward chaining example



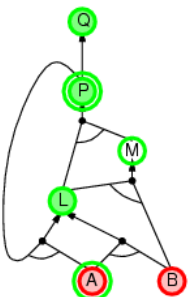
$P \Rightarrow Q$
 $L \wedge M \Rightarrow P$
 $B \wedge L \Rightarrow M$
 $A \wedge P \Rightarrow L$
 $A \wedge B \Rightarrow L$
 A
 B

Backward chaining example



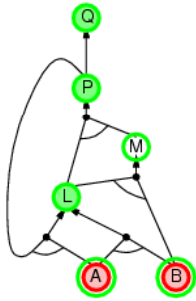
$P \Rightarrow Q$
 $L \wedge M \Rightarrow P$
 $B \wedge L \Rightarrow M$
 $A \wedge P \Rightarrow L$
 $A \wedge B \Rightarrow L$
 A
 B

Backward chaining example



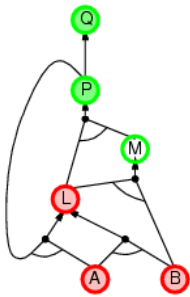
$P \Rightarrow Q$
 $L \wedge M \Rightarrow P$
 $B \wedge L \Rightarrow M$
 $A \wedge P \Rightarrow L$
 $A \wedge B \Rightarrow L$
 A
 B

Backward chaining example



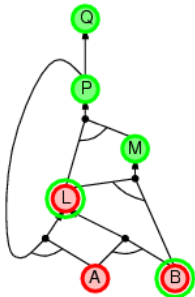
- $P \Rightarrow Q$
- $L \wedge M \Rightarrow P$
- $B \wedge L \Rightarrow M$
- $A \wedge P \Rightarrow L$
- $A \wedge B \Rightarrow L$
- A
- B

Backward chaining example

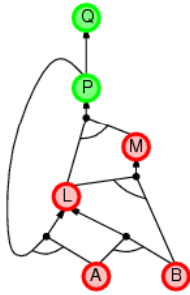


- $P \Rightarrow Q$
- $L \wedge M \Rightarrow P$
- $B \wedge L \Rightarrow M$
- $A \wedge P \Rightarrow L$
- $A \wedge B \Rightarrow L$
- A
- B

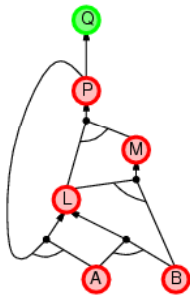
Backward chaining example



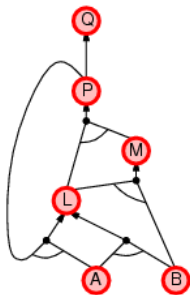
Backward chaining example



Backward chaining example



Backward chaining example



Prolog uses Backward Chaining

q :- p.
p :- l, m.
m :- b, l.
l :- a, p.
l :- a, b.
a.
b.

? q.
Yes.

Given:

$P \Rightarrow Q$
 $L \wedge M \Rightarrow P$
 $B \wedge L \Rightarrow M$
 $A \wedge P \Rightarrow L$
 $A \wedge B \Rightarrow L$
 A
 B

Is Q true?

Example of which to use

Prove that if n is an integer and n^3+5 is odd, then n is even

- Via direct proof
 - $n^3+5 = 2k+1$ for some integer k (definition of odd numbers)
 - $n^3 = 2k-4$
 - $n = \sqrt[3]{2k-4}$
- So direct proof didn't work out. Next up: indirect proof

29

Example of which to use

Prove that if n is an integer and n^3+5 is odd, then n is even

- Via indirect proof
 - Contrapositive: If n is odd, then n^3+5 is even
 - Assume n is odd, and show that n^3+5 is even
 - $n=2k+1$ for some integer k (definition of odd numbers)
 - $n^3+5 = (2k+1)^3+5 = 8k^3+12k^2+6k+6 = 2(4k^3+6k^2+3k+3)$
 - As $2(4k^3+6k^2+3k+3)$ is 2 times an integer, it is even

30

Proof by contradiction

- Given a statement p , assume it is false
 - Assume $\neg p$
- Prove that $\neg p$ leads to false
 - A contradiction exists
- Given a statement of the form $p \rightarrow q$
 - To assume it's false, you only have to consider the case where p is true and q is false

31

Proof by contradiction example 1

- Theorem (by Euclid): There are infinitely many prime numbers.
- Proof. Assume there are a finite number of primes
- List them as follows: p_1, p_2, \dots, p_n .
- Consider the number $q = p_1 p_2 \dots p_n + 1$
 - This number is not divisible by any of the listed primes
 - If we divided p_i into q , there would result a remainder of 1
 - We must conclude that q is a prime number, not among the primes listed above
 - This contradicts our assumption that all primes are in the list p_1, p_2, \dots, p_n .

32

Proof by contradiction example 2

Prove that if n is an integer and n^3+5 is odd, then n is even

Rephrased: If n^3+5 is odd, then n is even

• Thus, p is " n^3+5 is odd, q is " n is even"

- Assume p and $\neg q$
 - Assume that n^3+5 is odd, and n is odd
- Since n is odd:
 - $n=2k+1$ for some integer k (definition of odd numbers)
 - $n^3+5 = (2k+1)^3+5 = 8k^3+12k^2+6k+6 = 2(4k^3+6k^2+3k+3)$
 - As $n = 2(4k^3+6k^2+3k+3)$ is 2 times an integer, n must be even
 - Thus, we have concluded q
- Contradiction!
 - We assumed q was false, and showed that this assumption implies that q must be true
 - As q cannot be both true and false, we have reached our contradiction

33

A note on that problem...

Prove that if n is an integer and n^3+5 is odd, then n is even
Here, our implication is: If n^3+5 is odd, then n is even

- The indirect proof proved the contrapositive: $\neg q \rightarrow \neg p$
 - I.e., If n is odd, then n^3+5 is even
- The proof by contradiction assumed that the implication was false, and showed that led to a contradiction
 - If we assume p and $\neg q$, we can show that implies q
 - The contradiction is q and $\neg q$
- Note that both used similar steps, but are different means of proving the implication

34

Vacuous proofs

- Consider an implication: $p \rightarrow q$
- If it can be shown that p is false, then the implication is always true
 - By definition of an implication
- Note that you are showing that the antecedent is false

35

Vacuous proof example

- Consider the statement:
 - All criminology majors in 22c:19 are female
 - Rephrased: If you are a criminology major and you are in 22c:19, then you are female
 - Could also use quantifiers!
- Since there are no criminology majors in this class, the antecedent is false, and the implication is true

36

Trivial proofs

- Consider an implication: $p \rightarrow q$
- If it can be shown that q is true, then the implication is always true
 - By definition of an implication
- Note that you are showing that the conclusion is true

37

Trivial proof example

- Consider the statement:
 - If you are tall and are in 22c:19 then you are a student
- Since all people in 22c:19 are students, the implication is true regardless

38

Proof by cases

- Show a statement is true by showing all possible cases are true
- Thus, you are showing a statement of the form: $(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q$

is true by showing that:

$$[(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q)]$$

39

Proof by cases example

- Prove that $\frac{|a|}{|b|} = \frac{|a|}{|b|}$
 - Note that $b \neq 0$

- Cases:

- Case 1: $a \geq 0$ and $b > 0$

- Then $|a| = a$, $|b| = b$, and

$$\frac{|a|}{|b|} = \frac{a}{b} = \frac{|a|}{|b|}$$

- Case 2: $a \geq 0$ and $b < 0$

- Then $|a| = a$, $|b| = -b$, and

$$\frac{|a|}{|b|} = \frac{a}{-b} = \frac{a}{-b} = \frac{|a|}{|b|}$$

- Case 3: $a < 0$ and $b > 0$

- Then $|a| = -a$, $|b| = b$, and

$$\frac{|a|}{|b|} = \frac{-a}{b} = \frac{-a}{b} = \frac{|a|}{|b|}$$

- Case 4: $a < 0$ and $b < 0$

- Then $|a| = -a$, $|b| = -b$, and

$$\frac{|a|}{|b|} = \frac{-a}{-b} = \frac{-a}{-b} = \frac{|a|}{|b|}$$

40

The thing about proof by cases

- Make sure you get ALL the cases
 - The biggest mistake is to leave out some of the cases
- Don't have extra cases
 - We could have 9 cases in the last example
 - Positive numbers
 - Negative numbers
 - Zero
 - Those additional cases wouldn't have added anything to the proof

41

Proofs of equivalences

- This is showing the definition of a bi-conditional
- Given a statement of the form “p if and only if q”
 - Show it is true by showing $(p \rightarrow q) \wedge (q \rightarrow p)$ is true

42

Proofs of equivalence example

- Rosen, section 1.5, question 40
 - Show that $m^2=n^2$ if and only if $m=n$ or $m=-n$
 - Rephrased: $(m^2=n^2) \leftrightarrow [(m=n) \vee (m=-n)]$
- Need to prove two parts:
 - $[(m=n) \vee (m=-n)] \rightarrow (m^2=n^2)$
 - Proof by cases!
 - Case 1: $(m=n) \rightarrow (m^2=n^2)$
 - $(m)^2 = m^2$, and $(n)^2 = n^2$, so this case is proven
 - Case 2: $(m=-n) \rightarrow (m^2=n^2)$
 - $(m)^2 = m^2$, and $(-n)^2 = n^2$, so this case is proven
 - $(m^2=n^2) \rightarrow [(m=n) \vee (m=-n)]$
 - Subtract n^2 from both sides to get $m^2-n^2=0$
 - Factor to get $(m+n)(m-n) = 0$
 - Since that equals zero, one of the factors must be zero
 - Thus, either $m+n=0$ (which means $m=-n$) or $m-n=0$ (which means $m=n$)

43

Existence proofs

- Given a statement: $\exists x P(x)$
- We only have to show that a $P(c)$ exists for some value of c
- Two types:
 - Constructive: Find a specific value of c for which $P(c)$ exists
 - Nonconstructive: Show that such a c exists, but don't actually find it
 - Assume it does not exist, and show a contradiction

44

Constructive existence proof example

- Show that a square exists that is the sum of two other squares
 - Proof: $3^2 + 4^2 = 5^2$
- Show that a cube exists that is the sum of three other cubes
 - Proof: $3^3 + 4^3 + 5^3 = 6^3$

45

Non-constructive existence proof example

- Rosen, section 1.5, question 50
- Prove that either $2 \cdot 10^{500} + 15$ or $2 \cdot 10^{500} + 16$ is not a perfect square
 - A perfect square is a square of an integer
 - Rephrased: Show that a non-perfect square exists in the set $\{2 \cdot 10^{500} + 15, 2 \cdot 10^{500} + 16\}$
- Proof: The only two perfect squares that differ by 1 are 0 and 1
 - Thus, any other numbers that differ by 1 cannot both be perfect squares
 - Thus, a non-perfect square must exist in any set that contains two numbers that differ by 1
 - Note that we didn't specify which one it was!

46

Uniqueness proofs

- A theorem may state that only one such value exists
- To prove this, you need to show:
 - Existence: that such a value does indeed exist
 - Either via a constructive or non-constructive existence proof
 - Uniqueness: that there is only one such value

47

Uniqueness proof example

- If the real number equation $5x+3=a$ has a solution then it is unique
- Existence
 - We can manipulate $5x+3=a$ to yield $x=(a-3)/5$
 - Is this constructive or non-constructive?
- Uniqueness
 - If there are two such numbers, then they would fulfill the following: $a = 5x+3 = 5y+3$
 - We can manipulate this to yield that $x = y$
 - Thus, the one solution is unique!

48

Counterexamples

- Given a universally quantified statement, find a single example which it is not true
- Note that this is DISPROVING a UNIVERSAL statement by a counterexample
- $\forall x \neg R(x)$, where $R(x)$ means "x has red hair"
 - Find one person (in the domain) who has red hair
- Every positive integer is the square of another integer
 - The square root of 5 is 2.236, which is not an integer

49

A note on counterexamples

- You can DISPROVE something by showing a single counter example
 - You are finding an example to show that something is not true
- You cannot PROVE something by example
- Example: prove or disprove that all numbers are even
 - Proof by contradiction: 1 is not even
 - (Invalid) proof by example: 2 is even

50

Mistakes in proofs

- Modus Badus
 - Fallacy of denying the hypothesis
 - Fallacy of affirming the conclusion
- Proving a universal by example
 - You can only prove an existential by example!
- Disproving an existential by example
 - You can only disprove a universal by example!

51
