CS 173, Lecture B
August 27, 2015

Tandy Warnow

Proofs

- You want to prove that some statement A is true.
- You can try to prove it directly, or you can prove it indirectly… we'll show examples of each type of proof.

Example of direct proof

Theorem: Every odd integer is the difference of two perfect squares. (In other words, for all odd integers x, there exist integers y and z such that $x=y^2-z^2$.)

Example of direct proof

Theorem: Every odd integer is the difference of two perfect squares. (In other words, for all odd integers x, there exist integers y and z such that $x=y^2-z^2$.)

Proof. Since x is odd, there is an integer L such that

$x = 2L+1$.

Note that $x = (L^2+2L+1) – L^2 = (L+1)^2 – L^2$.

q.e.d.

A proof by contradiction

- Theorem: The square root of 7 is irrational.

A proof by contradiction

- Theorem: The square root of 7 is irrational.
- Proof: Let $x=\sqrt{7}$. We know that x is a real number. Hence, we will prove x is irrational by contradiction.

A proof by contradiction

- Theorem: The square root of 7 is irrational.
- Proof: Let $x=\sqrt{7}$. We know that x is a real number. Hence, we will prove x is irrational by contradiction.
- If x is rational, then $x = A/B$, where A and B are integers and $\gcd(A,B)=1$. Hence, A and B do not share any prime factors.

A proof by contradiction

- Theorem: The square root of 7 is irrational.
- Proof: Let $x=\sqrt{7}$. We know that x is a real number. Hence, we will prove x is irrational by contradiction.
- If x is rational, then $x = A/B$, where A and B are integers and gcd(A,B)=1. Hence, A and B do not share any prime factors.
- Then $x^2 = 7$. Hence $A^2/B^2 = 7$. Hence, $A^2 = 7B^2$.

A proof by contradiction

- Theorem: The square root of 7 is irrational.
- Proof: Let $x=\sqrt{7}$. We know that x is a real number. Hence, we will prove x is irrational by contradiction.
- If x is rational, then $x = A/B$, where A and B are integers and $\gcd(A,B)=1$. Hence, A and B do not share any prime factors.
- Then $x^2 = 7$. Hence $A^2/B^2 = 7$. Hence, $A^2 = 7B^2$.
- Hence 7 divides A^2.

A proof by contradiction

- Theorem: The square root of 7 is irrational.
- Proof: Let $x=\sqrt{7}$. We know that x is a real number. Hence, we will prove x is irrational by contradiction.
- If x is rational, then $x = A/B$, where A and B are integers and $\gcd(A,B)=1$. Hence, A and B do not share any prime factors.
- Then $x^2 = 7$. Hence $A^2/B^2 = 7$. Hence, $A^2 = 7B^2$.
- Hence 7 divides A^2.
- Hence 7 divides A.

A proof by contradiction

- Theorem: The square root of 7 is irrational.
- Proof: Let $x=\sqrt{7}$. We know that x is a real number. Hence, we will prove x is irrational by contradiction.
- If x is rational, then $x = A/B$, where A and B are integers and gcd(A,B)=1. Hence, A and B do not share any prime factors.
- Then $x^2 = 7$. Hence $A^2/B^2 = 7$. Hence, $A^2 = 7B^2$.
- Hence 7 divides A^2.
- Hence 7 divides A.
- Hence 7^2 divides $A^2 = 7B^2$

A proof by contradiction

- Theorem: The square root of 7 is irrational.
- Proof: Let $x=\sqrt{7}$. We know that x is a real number. Hence, we will prove x is irrational by contradiction.
- If x is rational, then $x = A/B$, where A and B are integers and gcd(A,B)=1. Hence, A and B do not share any prime factors.
- Then $x^2 = 7$. Hence $A^2/B^2 = 7$. Hence, $A^2 = 7B^2$.
- Hence 7 divides A^2.
- Hence 7 divides A.
- Hence 7^2 divides $A^2 = 7B^2$
- Hence 7 divides B^2. Hence 7 divides B.

A proof by contradiction

- Theorem: The square root of 7 is irrational.
- Proof: Let $x=\sqrt{7}$. We know that x is a real number. Hence, we will prove x is irrational by contradiction.
- If x is rational, then $x = A/B$, where A and B are integers and gcd(A,B)=1. Hence, A and B do not share any prime factors.
- Then $x^2 = 7$. Hence $A^2/B^2 = 7$. Hence, $A^2 = 7B^2$.
- Hence 7 divides A^2.
- Hence 7 divides A.
- Hence 7^2 divides $A^2 = 7B^2$
- Hence 7 divides B^2. Hence 7 divides B.
- Hence A and B are both divisible by 7, contradicting the assumptions above.

A proof by contradiction

- Theorem: The square root of 7 is irrational.
- Proof: Let $x=\sqrt{7}$. We know that x is a real number. Hence, we will prove x is irrational by contradiction.
- If x is rational, then $x = A/B$, where A and B are integers and gcd(A,B)=1. Hence, A and B do not share any prime factors.
- Then $x^2 = 7$. Hence $A^2/B^2 = 7$. Hence, $A^2 = 7B^2$.
- Hence 7 divides A^2.
- Hence 7 divides A.
- Hence 7^2 divides $A^2 = 7B^2$
- Hence 7 divides B^2. Hence 7 divides B.
- Hence A and B are both divisible by 7, contradicting the assumptions above.
- Therefore x must not be rational. Since we know x must be real, it follows that x must instead be irrational.

q.e.d

Brief introduction to sets

- A set S is just a collection of objects. Some sets are finite (e.g., {1,2,3,5}) and some are infinite (e.g., the set of integers, the set of functions from the integers to the open interval (0,1), etc.).
- We can specify a set explicitly, as in {1,2,3,5}, or implicitly, as in the "set-builder notation": {x in Z: 0 < x < 6, x != 4}. These are the same set, represented differently.
- We can also write {f: Z -> (0,1)} to denote the set of functions from the set of integers (Z) to the open interval (0,1).

Brief introduction to sets

- Notation:
  - For a set A, and element x of A, we can write
    - x ε A
    - And in latex we write "$x \in A$"
  - A set B where all elements of B are elements of A is called a "subset" of A. In latex we write this as
    - $B \subseteq A$
  - Note therefore that if x ε A then {x} is a subset of A.

Another proof by contradiction

- Theorem: Let A be a subset of the integers that satisfies the following constraint:
  - $x \in A \Rightarrow x+1 \in A$

Another proof by contradiction

- Theorem: Let A be a subset of the integers that satisfies the following constraint:
  - $x \in A \Rightarrow x+1 \in A$

  Then if A is finite, it follows that A is the empty set.

Another proof by contradiction

- Theorem: Let A be a subset of the integers that satisfies the following constraint:
  - $x \in A \Rightarrow x+1 \in A$

  Then if A is finite, it follows that A is the empty set.

Proof: Suppose A is not the empty set but is finite. Then $A = \{a_1, a_2, \ldots, a_n\}$ for some n

Another proof by contradiction

- Theorem: Let A be a subset of the integers that satisfies the following constraint:
  - $x \in A \Rightarrow x+1 \in A$

  Then if A is finite, it follows that A is the empty set.

Proof: Suppose A is not the empty set but is finite. Then $A = \{a_1, a_2, \ldots, a_n\}$ for some n. Let a* be the largest element in A.

.

Another proof by contradiction

- Theorem: Let A be a subset of the integers that satisfies the following constraint:
  - $x \in A \Rightarrow x+1 \in A$

  Then if A is finite, it follows that A is the empty set.

Proof: Suppose A is not the empty set but is finite. Then $A = \{a_1, a_2, \ldots, a_n\}$ for some n. Let a* be the largest element in A. Then by assumption, b= a*+1 is an element of A.

Another proof by contradiction

- Theorem: Let A be a subset of the integers that satisfies the following constraint:
  - $x \in A \Rightarrow x+1 \in A$

Then if A is finite, it follows that A is the empty set.

Proof: Suppose A is not the empty set but is finite. Then $A = \{a_1, a_2, \ldots, a_n\}$ for some n. Let a* be the largest element in A. Then by assumption, b= a*+1 is an element of A. But then b>a*, contradicting our hypothesis. Hence, A must not be finite.

Another proof by contradiction

- Theorem: Let A be a subset of the integers that satisfies the following constraint:
  - $x \in A \Rightarrow x+1 \in A$

  Then if A is finite, it follows that A is the empty set.

Proof. We have shown that if A is not the empty set, then A cannot be finite. We now want to show that it is possible for A to be the empty set.

Another proof by contradiction

- Theorem: Let A be a subset of the integers that satisfies the following constraint:
  - $x \in A \Rightarrow x+1 \in A$

  Then if A is finite, it follows that A is the empty set.

Proof. What happens if A is the empty set? Does A satisfy the constraint above?

Yes!!

Another proof by contradiction

- Theorem: Let A be a subset of the integers that satisfies the following constraint:
  - $x \in A \Rightarrow x+1 \in A$

  Then if A is finite, it follows that A is the empty set.

Proof. The constraint given above is the statement

$x \in A \Rightarrow x+1 \in A$

This is the same thing as saying

"whenever $x \in A$, it follows that $x+1 \in A$".

Or, equivalent,

"for all elements x of A, the real number x+1 is an element of A".

Or, "if x is an element of A, then x+1 is an element of A".

The only way this constraint can be violated is if there is *some* element x of A, where x+1 is not an element of A.

If A is the empty set, then this constraint can never be violated.

Note also – an "IF X THEN Y" statement cannot be False when X is False. The only way it can be false is if X is true and Y is false.

A logic problem

- Suppose we are in a city where there are two types of people – those who always tell the truth, and those who always lie.
  We meet two people, Sally and Tom, and we don't know if they are both liars, both truth tellers, or one of each.
  - Sally says: "Exactly one of us is telling the truth."
  - Tom says: "Sally is telling the truth."
- Determine who is telling the truth and who is lying (and prove your answer is correct).

Homework and discussion section

- Homework (due Monday, 10 PM, on Moodle):
  - Prove that the square root of 5 is irrational
  - Prove that there is no largest real number less than 1
- Discussion section problems
  - Prove that the square root of 11 is irrational
  - Prove that there is no smallest real number greater than 1
  - Suppose A is a finite subset of the real numbers that satisfies:
    - For all a in A, 2a is also an element of A.

    Find all the sets A that satisfy this constraint, and prove that there are no others. (Hint: there are only two such sets.)

NOTE: Homeworks are easier than discussion section problems. But over time, your ability to solve harder problems will increase, and then the homeworks will also become more challenging!

Logic

- Logical variables
- Propositions (statements that are true or false)
- Predicates (statements that are true or false, but depend on the variables)
- Quantifiers (for all, there exists)
- AND, OR, XOR,
- IF A THEN B, or A -> B
- IFF = IF AND ONLY IF
- NEGATION

A AND B

A and B are logical statements – each can be true or false, but only one

A AND B is true if and only if both are true

- W = “Today is Friday”
- X = “We are in Chicago”
- Y = “Today is Thursday”
- Z = “Barack Obama is the president of the USA”

Which of the following statements are true?

Y AND Z (two true statements)
X AND Y (one false, one true)
X AND Z (one false, one true)
W AND X (two false statements)

A OR B

A and B are logical statements – each can be true or false, but only one

A OR B is true if and only if one or both are true (i.e., if and only if at least one is true)

- W = “Today is Friday”
- X = “We are in Chicago”
- Y = “Today is Thursday”
- Z = “Barack Obama is the president of the USA”

Which of the following statements are true?

Y OR Z (two true statements)
X OR Y (one false, one true)
X OR Z (one false, one true)
W OR X (two false statements)

A XOR B

A and B are logical statements – each can be true or false, but only one

A XOR B is true if and only if exactly one of A and B is true
This is the same as the "exclusive OR"

- W = "Today is Friday"
- X = "We are in Chicago"
- Y = "Today is Thursday"
- Z = "Barack Obama is the president of the USA"

Which of the following statements are true?

Y XOR Z (two true statements)
X XOR Y (one false, one true)
X XOR Z (one false, one true)
W XOR X (two false statements)

IF A THEN B

A and B are logical statements – each can be true or false, but only one

IF A THEN B is true if and only if…

IF A THEN B

A and B are logical statements – each can be true or false, but only one

IF A THEN B is true if and only if…

Think about it.

IF A THEN B

- IF A THEN B is the same as
  - "whenever A, then always B"
  - "Not possible for B to be false if A is true"

- So, how would you *disprove* "If A THEN B"?

IF A THEN B

- IF A THEN B is the same as
  - "whenever A, then always B"
  - "Not possible for B to be false if A is true"

- To disprove "IF A THEN B", you would have to have A being True but B being false.

- Example: to disprove "If x=8 THEN y=5" show that "x=8" and "y != 5" is possible.

IF A THEN B

A and B are logical statements – each can be true or false, but only one

IF A THEN B is true if and only if … (A is false) OR (A is true and B is true)

IF A THEN B

A and B are logical statements – each can be true or false, but only one

IF A THEN B is true if and only if … (A is false) OR (A is true and B is true)

- W = “Today is Friday”
- X = “We are in Chicago”
- Y = “Today is Thursday”
- Z = “Barack Obama is the president of the USA”

IF A THEN B

A and B are logical statements – each can be true or false, but only one

IF A THEN B is true if and only if … (A is false) OR (A is true and B is true)

- W = “Today is Friday”
- X = “We are in Chicago”
- Y = “Today is Thursday”
- Z = “Barack Obama is the president of the USA”

Which of the following statements are true?

IF Y THEN Z (both true statements)
IF X THEN Z (X false, Z true)
IF Z THEN X (X false, Z true)
IF W THEN X (two false statements)

IF A THEN B

- Which of the following is true?
  1. IF Illinois is in the USA, THEN 2=1+1
  2. IF Illinois is in the USA, THEN 2=3
  3. IF 2=3 THEN Illinois is in the USA
  4. IF 2=3 THEN Illinois is not in the USA
  5. If (2=3 OR Illinois is in the USA) THEN 2=3
  6. If (2=3 OR Illinois is in the USA) then Illinois is in the USA
  7. If (2=3 AND Illinois is in the USA) then 2=3

quantifiers

- “For all” (written as an upside-down “A”)
- “There exists” (written as a backwards “E”)

The order matters! Think about the following two statements (differing only in the order of the quantifiation):

- For all integers x, there exists an integer y such that $x \leq y$
- There exists an integer y such that for all integers x, $x \leq y$

quantifiers

- For all integers x, there exists an integer y such that $x \leq y$
- There exists an integer y such that for all integers x, $x \leq y$

quantifiers

- For all integers x, there exists an integer y such that $x<y$
- There exists an integer y such that for all integers x, $x<y$

The first one is true! Proof: Let x be an arbitrary integer. Then let $y=x+1$. Clearly y is an integer, and $x \leq y$. (For that matter, setting $y=x$ also works!) Q.E.D.

quantifiers

- For all integers x, there exists an integer y such that $x \leq y$
- There exists an integer y such that for all integers x other than y, $x \leq y$

The second statement is false!

Proof (by contradiction). Suppose the second statement is true….

quantifiers

- There exists an integer y such that for all integers x, $x \leq y$

The second statement is false!

Proof (by contradiction). Suppose the second statement is true…. Then there is an integer y such that for all integers x, $x \leq y$. Let $x=y+1$. Note that x is an integer, and that $x>y$. Hence, it is not the case that $x \leq y$. This contradicts our hypothesis, and so the claim is false. Q.E.D.

Problems with written English

- English is not as precise as mathematics, so be careful about how you interpret it. Better to use mathematical notation *and* English.
- What does the following statements mean?
  - All dogs are not stupid

  Is this the same as “Not all dogs are stupid”? Or just “all dogs are smart”? (If not being stupid means being smart.)
- How about
  - All students in this class are not in Africa.
  - All students in this class are not women.
- Try to be careful with how you write English – not just in this class, of course.

More logic: Negation

- Negation – what is the opposite of a statement?
- What is the negation of (A OR B)?

More logic: Negation

- Negation – what is the opposite of a statement?
- What is the negation of (A OR B)?
  - NOT A AND NOT B

More logic: Negation

- Negation – what is the opposite of a statement?
- What is the negation of (A OR B)?
  - NOT A AND NOT B
- What is the negation of (A AND B)?

More logic: Negation

- Negation – what is the opposite of a statement?
- What is the negation of (A OR B)?
  - NOT A AND NOT B
- What is the negation of (A AND B)?
  - NOT A OR NOT B

More logic: Negation

- Negation – what is the opposite of a statement?
- What is the negation of (A OR B)?
  - NOT A AND NOT B
- What is the negation of (A AND B)?
  - NOT A OR NOT B
- What is the negation of (IF A THEN B)?

More logic: Negation

- Negation – what is the opposite of a statement?
- What is the negation of (A OR B)?
  - NOT A AND NOT B
- What is the negation of (A AND B)?
  - NOT A OR NOT B
- What is the negation of (IF A THEN B)?
  - A AND NOT B

Logic math symbols table

Symbol	Symbol Name	Meaning / definition	Example
$\cdot$	and	and	$x \cdot y$
$\wedge$	caret / circumflex	and	$x \wedge y$
$\&$	ampersand	and	$x \& y$
$+$	plus	or	$x + y$
$\vee$	reversed caret	or	$x \vee y$
$\vert$	vertical line	or	$x \vert y$
x'	single quote	not - negation	x'
$\overline{x}$	bar	not - negation	$\overline{x}$
$\neg$	not	not - negation	$\neg x$
$!$	exclamation mark	not - negation	$! x$
$\oplus$	circled plus / oplus	exclusive or - xor	

http://www.rapidtables.com/math/symbols/Logic_Symbols.htm

$\sim$	tilde	negation	$\sim x$
$\Rightarrow$	implies		
$\Leftrightarrow$	equivalent	if and only if (iff)	
$\leftrightarrow$	equivalent	if and only if (iff)	
$\forall$	for all		
$\exists$	there exists		
$\nexists$	there does not exists		
$\therefore$	therefore		
$\because$	because / since		

More logic

- Suppose A is a finite subset of the real numbers that satisfies
  - For all a in A, the number 2a is also in A
- What can A be? (Note – you cannot change the meaning of multiplication.)

More logic

- Henry and Allen are each of them either always lying or always telling the truth (but that doesn't mean both of them are liars or both of them are truth tellers… there could be one of each).
- Henry says "Allen is a truth teller"
- Allen says "Only one of us is a truth teller"

Is either a truth teller? If so, who?