

# CPSC 121: Models of Computation

## Unit 7: Proof Techniques

Based on slides by Patrice Belleville and Steve Wolfman

## Pre-Class Learning Goals

- By the start of class, for each proof strategy below, you should be able to:
  - Identify the form of statement the strategy can prove.
  - Sketch the structure of a proof that uses the strategy.
- Strategies for quantifiers:
  - generalizing from the generic particular (WLOG) (for  $\forall x \in Z \dots$ )
  - constructive/non-constructive proofs of existence (for  $\exists x \in Z \dots$ )
  - proof by exhaustion (for  $\forall x \in Z \dots$ )
- General strategies
  - antecedent assumption proof (for  $p \rightarrow q$ .)
  - proof by contrapositive (for  $p \rightarrow q$ .)
  - proof by contradiction (for any statement.)
  - proof by cases. (for any statement.)

Unit 7- Proof Techniques

2

## Quiz 7 Feedback:

- In general :
- Issues:

- We will do more proof examples in class.

Unit 7- Proof Techniques

3

## Quiz 7 Feedback

- Open-ended question: when should you switch strategies?
  - When you are stuck.
  - When the proof is going around in circles.
  - When the proof is getting too messy.
  - When it is taking too long.
  - Through experience (how do you get that?)

Monitor yourself

Unit 7- Proof Techniques

4

## In-Class Learning Goals

- By the end of this unit, you should be able to:
  - Devise and attempt multiple different, appropriate proof strategies for a given theorem, including
    - all those listed in the "pre-class" learning goals
    - logical equivalences,
    - propositional rules of inference
    - rules of inference on quantifiers
  - i.e. be able to apply the strategies listed in the [Guide to Proof Strategies](#) reference sheet on the course web site (in Other Handouts)
  - For theorems requiring only simple insights beyond strategic choices or for which the insight is given/hinted, additionally prove the theorem.

## ? Where We Are in The BIG Questions ?

- How can we convince ourselves that an algorithm does what it's supposed to do?
  - We need to prove its correctness.
- How do we determine whether or not one algorithm is better than another one?
  - Sometimes, we need a proof to convince someone that the number of steps of our algorithm is what we claim it is.

## Unit Outline

- **Techniques for quantifiers.**
  - **Existential quantifiers.**
  - Universal quantifiers.
- Dealing with multiple quantifiers.
- Proof by contrapositive and contradiction
- Additional Examples

NOTE:  
Epp calls some of these direct proofs and others indirect. We'll avoid using these terms

## Techniques for quantifiers

- There are two general forms of statements:
  - Those that start with an existential quantifier.
  - Those that start with a universal quantifier.
- We use different techniques for them. We'll study each case in turns.

## Existential Statements

Suppose the statement has the form :

$$\exists x \in D, P(x)$$

- To prove this statement is true, we must
  - Find a value of  $x$  (a “witness”) for which  $P(x)$  holds.
- We call it a **witness proof**
- So the proof will look like this:
  - Let  $x = \langle \text{some value in } D \rangle$
  - Verify that the  $x$  we chose satisfies the predicate.
- Example: *There is a prime number  $x$  such that  $3x+2$  is not prime.*

## Existential Statements (cont')

- How do we translate *There is a prime number  $x$  such that  $3x+2$  is not prime* into predicate logic?
- A.  $\forall x \in \mathbb{Z}^+, \text{Prime}(x) \wedge \sim \text{Prime}(3x+2)$
- B.  $\exists x \in \mathbb{Z}^+, \text{Prime}(x) \wedge \sim \text{Prime}(3x+2)$**
- C.  $\forall x \in \mathbb{Z}^+, \text{Prime}(x) \rightarrow \sim \text{Prime}(3x+2)$
- D.  $\exists x \in \mathbb{Z}^+, \text{Prime}(x) \rightarrow \sim \text{Prime}(3x+2)$
- E. None of the above.

## Existential Statements (cont')

- What is the right start of the proof for the statement *There is a prime number  $x$  such that  $3x+2$  is not prime?*
- A. Without loss of generality let  $x$  be a positive integer ....
- B. Without loss of generality let  $x$  be a prime ....
- C. Let  $x$  be any non specific prime .....
- D. Let  $x$  be 2 .....**
- E. None of the above.

## Existential Statements (cont')

- So the proof goes as follows:

➤ Proof:

- Let  $x = 2$
- It is prime because its only factors are 1 and 2
- Now  $3x+2 = 2 * 2 + 2 = 8$   
and
- Hence  $3x+2$  is not prime.
- QED.

8 is not prime  
because  $8 = 2*4$

## Unit Outline

- Techniques for quantifiers.
  - Existential quantifiers.
  - **Universal quantifiers.**
- Dealing with multiple quantifiers.
- Proof by contrapositive and contradiction
- Additional Examples

## Universal Statements

Suppose our statement has the form :

$$\forall x \in D, P(x)$$

- To prove this statement is true, we must
  - Show that  $P(x)$  holds no matter how we choose  $x$ .
- So the proof will look like this:
  - Without loss of generality, let  $x$  be any element of  $D$  (or an equivalent expression like those shown on next page)
  - Verify that the predicate  $P$  holds for this  $x$ .
    - Note: the only assumption we can make about  $x$  is the fact that it belongs to  $D$ . So we can only use properties common to all elements of  $D$ .

## Universal Statements (cont')

- Terminology: the following statements all mean the same thing:
  - Let  $x$  be a nonspecific element of  $D$
  - Let  $x$  be an unspecified element of  $D$
  - Let  $x$  be an arbitrary element of  $D$
  - Let  $x$  be a generic element of  $D$
  - Let  $x$  be any element of  $D$
  - Suppose  $x$  is a particular but arbitrarily chosen element of  $D$ .

## Universal Statements (cont')

- Example: *Every Racket function definition is at least 12 characters long.*
- What is the starting phrase of a proof for this statement?
  - A. Without loss of generality let  $f$  be a string of 12 characters ....
  - B.** Let  $f$  be a nonspecific Racket function definition....
  - C. Let  $f$  be the following Racket function definition .....
  - D. Let  $f$  be a nonspecific Racket function with 12 or more characters ....
  - E. None of the above.

## Universal Statements (cont')

■ Example 1: *Every Racket function definition is at least 12 characters long.*

■ The proof goes as follows:

➤ Proof:

○ Let f be A non-specific Racket func. def.

○ Then f should look like:

(define (n) b),  
where n and b are strings with at  
least 1 character

○ Therefore f is at least 12 characters long.

## Universal Statements (cont')

Example 2: *The sum of two odd numbers is even.*

■ If  $\text{Odd}(x) \equiv \exists k \in \mathbb{N}, x = 2k+1$   
 $\text{Even}(x) \equiv \exists k \in \mathbb{N}, x = 2k$

the above statement is:

Proof:

Let n be an arbitrary natural number.  
Let m be an arbitrary natural number.  
Assume that n and m are both odd.  
Then,  $n = 2i + 1$  and  $m = 2j + 1$   
Then,  $m+n = 2(i + j + 1)$   
 $i + j + 1$  is even, so thus is  $n + m$ .

## Special Case : Antecedent Assumption

Suppose the statement has the form:

$$\forall x \in D, P(x) \rightarrow Q(x)$$

■ This is a special case of the previous formula

■ The textbook calls this (and only this) a direct proof.

■ The proof looks like this:

➤ Proof:

○ Consider an unspecified element k of D.

○ Assume that  $P(k)$  is true.

○ Use this and properties of the element of D to verify that the predicate Q holds for this k.

## Antecedent Assumption (cont')

■ Why is the line *Assume that  $P(k)$  is true* valid?

- A Because these are the only cases where  $Q(k)$  matters.
- B. Because  $P(k)$  is preceded by a universal quantifier.
- C. Because we know that  $P(k)$  is true.
- D. Both (a) and (c)
- E. Both (b) and (c)

## Antecedent Assumption (cont')

- Example: prove that
  - $\forall n \in \mathbb{N}, n \geq 1024 \rightarrow 10n \leq n \log_2 n$
- Proof:
  - WLOG let  $n$  be an unspecified natural number.
  - Assume that  $n \geq 1024$
  - Then
    - $n \geq 2^{10}$
    - $\log_2(n) \geq 10 \log_2(2)$
    - $\log_2(n) \geq 10$
    - $n \log_2(n) \geq 10n$

## ... and for fun ...

- Other interesting proof techniques ☺
  - Proof by intimidation
  - Proof by lack of space (Fermat's favorite!)
  - Proof by authority
  - Proof by never-ending revision
- For the full list, see:
  - <http://school.maths.uwa.edu.au/~berwin/humour/invalid.proofs.html>

## Unit Outline

- Techniques for direct proofs.
  - Existential quantifiers.
  - Universal quantifiers.
- **Dealing with multiple quantifiers.**
- Proof by contrapositive and contradiction
- Additional Examples

## Multiple Quantifiers

- How do we deal with theorems that involve multiple quantifiers?
  - Start the proof from the outermost quantifier.
  - Work our way inwards.
- Example:
  - *For every positive integer  $n$ , there is a prime  $p$  that is larger than  $n$ .*
  - Defining:  
 $\text{Prime}(x) \equiv \forall r \in \mathbb{Z}^+, \forall s \in \mathbb{Z}^+, x = rs \rightarrow (r=1 \wedge s=x) \vee (r=x \wedge s=1)$
  - The statement in predicate logic is:

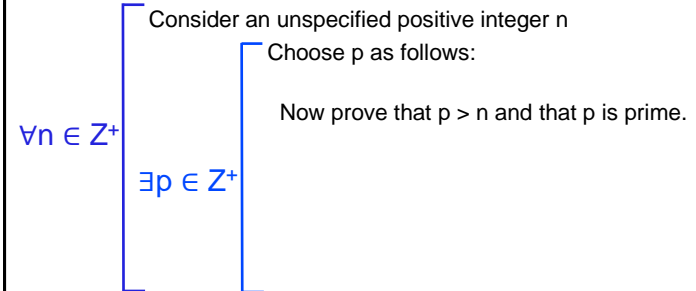
## Multiple Quantifiers: Example

- *Theorem: For every positive integer  $n$ , there is a prime  $p$  that is larger than  $n$ .*
- Which of the following is the predicate logic translation of the theorem?
  - A.  $\forall n \in \mathbb{Z}^+, \exists p \in \mathbb{Z}^+, \text{Prime}(p) \rightarrow p > n$
  - B.  $\forall n \in \mathbb{Z}^+, \forall p \in \mathbb{Z}^+, \text{Prime}(p) \rightarrow p > n$
  - C.  $\forall n \in \mathbb{Z}^+, \exists p \in \mathbb{Z}^+, \text{Prime}(p) \wedge p > n$
  - D.  $\forall n \in \mathbb{Z}^+, \forall p \in \mathbb{Z}^+, \text{Prime}(p) \wedge p > n$
  - E. None of the above.

## Multiple Quantifiers: Example

- The proof goes as follows:

➤ Proof:



## Multiple Quantifiers: Example

- How do we choose  $p$ ?
  - First we set  $x = n! + 1$  (where  $n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$ ).
  - By the fundamental theorem of arithmetic,  $x$  can be written as a product of primes:  
 $x = p_1 \cdot p_2 \cdots p_t$
  - We use any one of these as  $p$  (say  $p_1$ ).
- The integer  $p$  is a prime by definition.

## Multiple Quantifiers: Example

- Now we need to prove that  $p > n$ .
- Which of the following should we prove?
  - A.  $\forall i \in \mathbb{Z}^+, (2 \leq i \wedge i \leq n) \rightarrow i \text{ divides } n!$
  - B.  $\exists i \in \mathbb{Z}^+, 2 \leq i \wedge i \leq n \wedge i \text{ does not divide } x$
  - C.  $\forall i \in \mathbb{Z}^+, (2 \leq i \wedge i \leq p) \rightarrow i \text{ does not divide } x$
  - D.  $\forall i \in \mathbb{Z}^+, (2 \leq i \wedge i \leq n) \rightarrow i \text{ does not divide } x$
  - E. None of the above.

## Multiple Quantifiers: Example

### ■ Now the proof:

Let  $i$  be any unspecified integer such that  $2 \leq i \leq n$ .

Observe that

$$x/i = (n! + 1) / i = n! / i + 1/i = 1 \cdot 2 \cdots (i-1) \cdot (i+1) \cdots n + 1/i$$

Since  $1 \cdot 2 \cdots (i-1) \cdot (i+1) \cdots n$  is an integer, but  $1/i$  is not an integer, this means that  $x/i$  is not an integer.

Hence  $i$  does not divide  $x$ .

Therefore every factor of  $x$  is greater than  $n$

And  $p > n$

## Multiple Quantifiers: Example 2

### ■ Another example:

*Every even square can be written as the sum of two consecutive odd integers.*

or

$$\forall x \in \mathbb{Z}^+, \text{Even}(x) \wedge \text{Square}(x) \rightarrow \text{SumOfTwoConsOdd}(x)$$

### ■ Where :

➤  $\text{Square}(x) \equiv \exists y \in \mathbb{Z}^+, x = y^2$

➤  $\text{SumOfTwoConsOdd}(x) \equiv \exists k \in \mathbb{Z}^+, x = (2k-1) + (2k+1)$

### ■ Prove it using the following theorem:

*For every positive integer  $n$ , if  $n^2$  is even, then  $n$  is even.*

## Multiple Quantifiers: Example 2

### ■ Proof:

- Consider an unspecified integer  $x$
- Assume that  $x$  is an even square.

Therefore  $x$  can be written as the sum of two consecutive odd integers.

## Unit Outline

### ■ Techniques for direct proofs.

➤ Existential quantifiers.

➤ Universal quantifiers.

### ■ Dealing with multiple quantifiers.

### ■ **Proof by contrapositive and contradiction**

### ■ Additional Examples



## Contrapositive

- Consider the following theorem:

*If the square of a positive integer  $n$  is even, then  $n$  is even.*

- How can we prove this?

- Let's try a direct proof.

Consider an unspecified integer  $n$ .

Assume that  $n^2$  is even.

So  $n^2 = 2k$  for some (positive) integer  $k$ .

Hence  $n = \sqrt{2k}$

Then what?

## Contrapositive

- Consider instead the following theorem:

*If a positive integer  $n$  is odd, then its square is odd.*

- We can prove this easily:

Consider an unspecified positive integer  $n$ .

Assume that  $n$  is odd.

Hence  $n = 2k+1$  for some integer  $k$ .

Then  $n^2 = (2k+1)^2$

$$= 4k^2 + 4k + 1$$

$$= 2(2k^2+2k)+1$$

$$= 2m+1$$

where  $m = 2k^2+2k$

Therefore  $n^2$  is odd.

## Contrapositive

- What is the relationship between

*If the square of a positive integer  $n$  is even, then  $n$  is even.*

and

*If a positive integer  $n$  is odd, then its square is odd.*

?

- They are

- and hence

## Proof by Contradiction

- To prove:

Premise 1

...

Premise  $n$

Conclusion

- We assume Premise 1, ..., Premise  $n$ ,  $\sim$ Conclusion and then derive a contradiction

( i.e.  $p \wedge \sim p$ ,  $x$  is odd  $\wedge x$  is even,  $x < 5 \wedge x > 10$ , etc).

- We then conclude that Conclusion is true.

## Proof by Contradiction

### ■ Why are proofs by contradiction a valid proof technique?

- We proved  
 $\text{Premise } 1 \wedge \dots \wedge \text{Premise } n \wedge \sim \text{Conclusion} \rightarrow F$
- By the definition of  $\rightarrow$  this is equivalent to  
 $\sim(\text{Premise } 1 \wedge \dots \wedge \text{Premise } n \wedge \sim \text{Conclusion}) \vee F$
- By the identity law it is equivalent to  
 $\sim(\text{Premise } 1 \wedge \dots \wedge \text{Premise } n \wedge \sim \text{Conclusion})$
- By De Morgan :  
 $\sim(\text{Premise } 1 \wedge \dots \wedge \text{Premise } n) \vee \text{Conclusion}$
- By the definition of  $\rightarrow$  :  
 $\text{Premise } 1 \wedge \dots \wedge \text{Premise } n \rightarrow \text{Conclusion}$

## Proof by Contradiction: Example 1

### ■ Example:

*Not every CPSC 121 student got an above average grade on midterm 1.*

### ■ What are:

- The premise(s)?
- The negated conclusion?

### ■ Let us prove this theorem together.

## Proof by Contradiction: Example 2

### ■ Example :

*A group of CPSC 121 students show up in a room for a tutorial. The TA is late, and so the students start talking to each other. If every student has talked to at least one other student, then two of the students talked to exactly the same number of people.*

### ■ What are

- the premise(s)?
- the negated conclusion?

### ■ Prove the theorem!

## Proof by Contradiction: Example 3

### ■ Another example:

*Prove that for all real numbers  $x$  and  $y$ , if  $x$  is a rational number, and  $y$  is an irrational number, then  $x+y$  is irrational.*

### ■ What are

- the premise(s)?
- the negated conclusion?

### ■ Prove the theorem!

## How should you tackle a proof?

- Try the simpler methods first:
  - Witness proofs (if applicable).
  - Generalizing from the generic particular.
  - Proof by contrapositive.
  - Proof by contradiction.
  - Proof by cases
- If you don't know if the theorem is true:
  - Alternate between trying to prove and disprove it.
  - Use a failed attempt at one to help with the other.

## How should you tackle a proof? (cont')

- If you get stuck, try looking backwards from the conclusion you want.
  - But don't forget the argument must eventually be written from the premises to the conclusion (not the other way around).
- Try to derive all new facts you can derive from the premises without worrying about whether or not they will help.
- If you are really stuck, take a break, discuss it with some one, ask for help!


## Unit Outline

- Techniques for direct proofs.
  - Existential quantifiers.
  - Universal quantifiers.
- Dealing with multiple quantifiers.
- Indirect proofs: contrapositive and contradiction
- **Additional Examples**

## Exercises

- Prove that for every positive integer  $x$ , either  $\sqrt{x}$  is an integer, or it is irrational.
- Prove that any circuit consisting of NOT, OR, AND and XOR gates can be implemented using only NOR gates.
- Prove that if  $a$ ,  $b$  and  $c$  are integers, and  $a^2 + b^2 = c^2$ , then at least one of  $a$  and  $b$  is even. Hint: use a proof by contradiction, and show that 4 divides both  $c^2$  and  $c^2 - 2$ .
- Prove that there is a positive integer  $c$  such that  $x + y \leq c \cdot \max\{x, y\}$  for every pair of positive integers  $x$  and  $y$ .

## Quiz 8



- Due Day and Time: Check the announcements
- Reading for Quiz 8:
  - Epp, 4th edition: 12.2, pages 791 to 795.
  - Epp, 3rd edition: 12.2, pages 745 to 747, 752 to 754
  - Rosen, 6th edition: 12.2 pages 796 to 798, 12.3
  - Rosen, 7th edition: 13.2 pages 858 to 861, 13.3