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 $\forall x \in Z \ldots$)
  - constructive/non-constructive proofs of existence (for $\exists x \in Z \ldots$)
  - proof by exhaustion (for $\forall x \in Z \ldots$)
- 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.)

Quiz 7 Feedback:

- In general :
- Issues:
- We will do more proof examples in class.

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

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
    - o all those listed in the "pre-class" learning goals
    - o logical equivalences,
    - o propositional rules of inference
    - o 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.
- Using logical equivalencies : Proof by contrapositive
- Using Premises
- Proof by 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:
  - o Those that start with an existential quantifier.
  - o 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 = <some value in D>
  - 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. $\forall x \in Z^+$, Prime(x) ∧ ~Prime(3x+2)
  - B. $\exists x \in Z^+$, Prime(x) ∧ ~Prime(3x+2)
  - C. $\forall x \in Z^+$, Prime(x) → ~Prime(3x+2)
  - D. $\exists x \in Z^+$, Prime(x) → ~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:
    - o Let x =
    - o It is prime because its only factors are 1 and
    - o Now 3x+2 =
      and
    - o Hence 3x+2 is not prime.
    - o QED.

Unit Outline

- Techniques for direct proofs.
  - Existential quantifiers.
  - **Universal quantifiers.**
- Dealing with multiple quantifiers.
- Using logical equivalencies : Proof by contrapositive
- Using Premises
- Proof by 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
    - Then f should look like:
    - Therefore f is at least 12 characters long.

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
  - $\forall n \in N,\ n \geq 1024 \rightarrow 10n \leq n\log_2 n$
- Proof:
  - WLOG let n be an unspecified natural number.
  - Assume that
  - Then

Antecedent Assumption (cont')

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

- If Odd(x) ≡ ∃k ∈ N, x = 2k+1
  Even(x) ≡ ∃k ∈ N, x = 2k

  the above statement is:

  $\forall n \in N, \forall m \in N, Odd(n) \wedge Odd(m) \rightarrow Even(n+m)$

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 for some natural number i, and
  m = 2i+1 for some natural number j
- Then m+n = 2i+1 + 2j+1 = 2i + 2j + 2 = 2(i+j+1)
- Since i+j+1 is a natural number, 2(i+j+1) is even and so is n+m.
- QED

… 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**.
- Using logical equivalencies : Proof by contrapositive
- Using Premises
- Proof by 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: Suppose we wan to prove:

  An algorithm whose run time is $t(n) = n^2$ is generally faster than an algorithm whose time is 60n, i.e. we want to show that as n increases, $60n < n^2$

  - The statement in predicate logic is:

    $$\exists i \in Z^+, \forall n \in Z^+, n \geq i \rightarrow 60n < n^2$$

Multiple Quantifiers: Example

- *Theorem:* $\exists i \in Z^+,\ \forall n \in Z^+,\ n \geq i \rightarrow 60n < n^2$
- We can think of it as a statement of the form

  $\exists i \in Z^+,\ P(i),$

  where $P(i) \equiv \forall n \in Z^+,\ n \geq i \rightarrow 60n < n$
- So, how do we pick i
  - A. Let i be any specific integer.
  - B. Without loss of generality, let i be any arbitrary positive integer
  - C. Let i = (a specific value)
  - D. None of the above

Multiple Quantifiers: Example

- *Theorem:* $\exists i \in Z^+,\ \forall n \in Z^+,\ n \geq i \rightarrow 60n < n^2$
- We can think of it as a statement of the form

  $\exists i \in Z^+,\ P(i),$

  where

  $P(i) \equiv \forall n \in Z^+,\ n \geq i \rightarrow 60n < n$
- So,

  We pick **i** = ??.

  LEAVE this blank until you know what to pick. Take notes as you learn more about **i**.

  Then, we prove: $\forall n \in Z^+,\ n \geq i \rightarrow 60n < n^2.$

Multiple Quantifiers: Example

- *Theorem:* $\exists i \in Z^+,\ \forall n \in Z^+,\ n \geq i \rightarrow 60n < n^2$
- *Proof:*
  - Let **i** = ??.
  - Need to prove $\forall n \in Z^+,\ n \geq i \rightarrow 60n < n^2$
- How do we proceed?
  - A. Let n = 10
  - B. Let n = 70
  - C. WLOG, let n be an arbitrary positive integer
  - D. Let n be some specific integer (we can decide later)
  - E. None of the above

Multiple Quantifiers: Example

- Theorem: $\exists i \in Z+,\ \forall n \in Z+,\ n \geq i \rightarrow 60n < n^2$
- Proof:
  - Let i = ??.
  - WLOG, let n be any arbitrary positive integer
  - Need to prove $n \geq i \rightarrow 60n < n^2$
- How should we prove this statement?
  - A. Pick an n value, like 100, and show that this is true.
  - B. Assume $n \geq i$ and prove $60n < n^2$.
  - C. Use proof by exhaustion and show that it is true for every n
  - D. We should use some other strategy.

Multiple Quantifiers: Example

- Theorem: $\exists i \in Z+, \forall n \in Z+, n \geq i \rightarrow 60n < n^2$
- Proof:
  - Let $i = ??$.
  - Let n be any arbitrary positive integer
  - Assume $n \geq i$
  - Then prove $60n < n^2$
- How do we prove inequalities?

“Rules” for Inequalities

Proving an inequality is a lot like proving equivalence.

First, do your scratch work (often solving for a variable).

Then, rewrite formally:

- Start from one side.
- Work step-by-step to the other.
- Never move “opposite” to your inequality (so, to prove “<”, never make the quantity smaller).
- Strict inequalities (< and >): have **at least one** strict inequality step.

Multiple Quantifiers: Example

- Theorem: $\exists i \in Z+, \forall n \in Z+, n \geq i \rightarrow 60n < n^2$
- Proof:
  - Let $i = ??$.
  - Let n be any arbitrary positive integer
  - Assume $n \geq i$
  - Then prove $60n < n^2$
- We need to pick an i, so that $60n < n^2$
  - Let’s solve this inequality for n: in our scratch work
  - So the solution is n>60. What i should be?

Multiple Quantifiers: Example

- Theorem: $\exists i \in Z+, \forall n \in Z+, n \geq i \rightarrow 60n < n^2$
- Proof:
  - Let **$i = 61$**.
  - Let n be any arbitrary positive integer
  - Assume $n \geq i$
  - Then

$$\begin{aligned} 60n &< 61n \\ &= i * n \\ &\leq n * n \quad \text{since } n \geq i \quad \text{(using the assumption)} \\ &= n^2 \end{aligned}$$

How Did We Build the Proof?

- Theorem: $\exists i \in Z+, \forall n \in Z+, n \geq i \rightarrow 60n < n^2$
- Proof:
  - Let **i = 61**.
  - Let n be any arbitrary positive integer
  - Assume $n \geq i$
  - Then

$$
\begin{aligned}
60n &< 61n \\
&= i * n \\
&\leq n * n \quad \text{since } n \geq i \quad \text{(using the assumption)} \\
&= n^2
\end{aligned}
$$

Unit Outline

- Techniques for direct proofs.
  - Existential quantifiers.
  - Universal quantifiers.
- Dealing with multiple quantifiers.
- **Using logical equivalencies : Proof by contrapositive**
- Using Premises
- Proof by contradiction
- Additional Examples

Using Logical Equivalences

- Every logical equivalence that we've learned applies to predicate logic statements.
- For example, to prove $\sim\exists x \in D, P(x)$, you can prove $\forall x \in D, \sim P(x)$ and then convert it back with generalized De Morgan's.
- To prove $\forall x \in D, P(x) \rightarrow Q(x)$, you can prove $\forall x \in D, \sim Q(x) \rightarrow \sim P(x)$ and convert it back using the contrapositive rule.

- In other words, Epp's "proof by contrapositive" is direct proof after applying a logical equivalence rule.

Example: 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 directly.

  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 contrapositive statement:
  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 $m = 2k^2+2k$
  Since k is an integer, $2k^2+2k$ is an integer and therefore n^2 is odd.

Contrapositive

- Since we proved the statement
  If a positive integer n is odd, then its square is odd.
  the contrapositive of this statement, i.e.
  If the square of a positive integer n is even, then n is even.
  is also true (by the propositional equivalence rules).

Unit Outline

- Techniques for direct proofs.
  - Existential quantifiers.
  - Universal quantifiers.
- Dealing with multiple quantifiers.
- Using logical equivalencies : Proof by contrapositive
- **Using Premises**
- Proof by contradiction
- Additional Examples

Using Premises: Universals

- What can you say if you know (you have already proven or its given)
  $\forall x \in D, P(x)$?
- If you know $\forall x \in D, P(x)$:
  You can say $P(d)$ is true for any particular d in D of your choice, for an arbitrary d, or for every d.
- This is basically the opposite of how we go about *proving* a universal. This is how we USE (instantiate) a universal statement.

Using Premises: Existentials

- What can you say if you know (you have already proven or its given)
  $\exists y \in D, Q(y)$?
- If you know $\exists y \in D, Q(y)$:
  Do you know Q(d) is true for every d in D?
  Do you know Q(d) is true for a particular d of your choice?

  What do you know?
- This is basically the opposite of how we go about *proving* an existential. This is how we USE (instantiate) an existential statement.

Using Predicate Logic Premises

- What can you say if you know (rather than needing to prove)
  $\forall x \in D, P(x)$ or $\exists y \in D, Q(y)$?
- If you know $\forall x \in D, P(x)$, you can say that
  - for any d in D that P(d) is true
  - P(d) is true for any particular d in D or for an arbitrary one.
- If you know $\exists y \in D, Q(y)$, you can say that
  - for some d in D, Q(d) is true, but you don't know which one
  - So, assume nothing more about e than that it's from D.

Example 1

- Suppose we know (factorization of integers theorem):
  For every integer n>1 there are distinct prime numbers $p_1, p_2, \ldots, p_k$ and integers $e_1, e_2, \ldots, e_k$ such that
  $n = p_1^{e1}\, p_2^{e2} \ldots\ p_k^{ek}$
- Prove:
  Every integer greater than 1 has at least one prime factor.
- What proof shall we do?
  A. Witness
  B. WLOG
  C. Antecedent assumption
  D. Contraposition
  E. I have no idea

Example 1

- Suppose we know (factorization of integers theorem):
  For every integer n>1 there are distinct prime numbers $p_1, p_2, \ldots, p_k$ and integers $e_1, e_2, \ldots, e_k$ such that
  $n = p_1^{e1}\, p_2^{e2} \ldots\ p_k^{ek}$
- Prove:
  Every integer greater than 1 has at least one prime factor.
- Proof:
  - WLOG let m be any integer greater than 1.
  - How shall we use the theorem?

Example 1

- Suppose we know (factorization of integers theorem):
  For every integer n>1 there are distinct prime numbers $p_1, p_2, \ldots, p_k$ and integers $e_1, e_2, \ldots, e_k$ such that
  $n = p_1^{e1}\, p_2^{e2} \ldots\; p_k^{ek}$
- Prove:
  Every integer greater than 1 has at least one prime factor.
- Proof:
  - WLOG let m be any integer greater than 1.
  - By the factorization theorem,
    $m = p_1^{e1}\, p_2^{e2} \ldots\; p_k^{ek}$
    for some primes $p_1, p_2, \ldots, p_k$ and integers $e_1, e_2, \ldots, e_k$.
  - Therefore m has at least one prime factor.

Example 2

- Another example:
  Every even square can be written as the sum of two consecutive odd integers.
  or
  $\forall x \in Z^+$, Even(x) $\wedge$ Square(x) $\rightarrow$ SumOfTwoConsOdd(x)
- Where :
  - Square(x) $\equiv$ $\exists y \in Z^+$, $x = y\, y$
  - SumOfTwoConsOdd(x) $\equiv$ $\exists k \in Z^+$, $x = (2k-1) + (2k+1)$
- Prove it using the following theorem:
  For every positive integer n, if n^2 is even, then n is even.

Example 2

- Proof:
  - Let x be any unspecified positive integer
  - Assume that x is an even square.
  - Then
    $x = y*y$ for some $y \in Z^+$ (1)
  - By the given theorem, y is even.
  - Therefore
    $y = 2m$ for some $m \in Z^+$ (2)
  - Then from (1) and (2) :
    $x = 2m * 2m = 4m^2$
    $= 2m^2 -1 + 2m^2 +1 = (2m^2 -1) + (2m^2 +1)$
  - Since m^2 is a positive integer then $2m^2 -1$ and $2m^2 +1$ are consecutive odd integers .
  - QED

Unit Outline

- Techniques for direct proofs.
  - Existential quantifiers.
  - Universal quantifiers.
- Dealing with multiple quantifiers.
- Using logical equivalencies : Proof by contrapositive
- Using Premises
- **Proof by contradiction**
- Additional Examples

Proof by Contradiction

- To prove p:

  Assume ~p.

  Derive a contradiction
  (i.e. p ^ ~p, x is odd ^ x is even, x < 5 ^ x > 10, etc).
- We have then shown that there was something wrong (impossible) about assuming ~p; so, p must be true.

- This is the same as antecedent assumption.

  We have proved **~p → F**

  What is the logical equivalent to it?

Proof by Contradiction: With premisses

- To prove:

  Premise_1

  ...

  Premise_n

  Conclusion

- We assume

  Premise_1, ..., Premise_n, ~Conclusion

  and then derive a contradiction
- We then conclude that Conclusion is true.

Proof by Contradiction

- Why are proofs by contradiction a valid proof technique?
  - We proved

    Premise 1 ∧ ... ∧ Premise n ∧ ~Conclusion → F
  - By the definition of → this is equivalent to

    ~(Premise 1 ∧ ... ∧ Premise n ∧ ~Conclusion) ∨ F
  - By the identity law it is equivalent to

    ~(Premise 1 ∧ ... ∧ Premise n ∧ ~Conclusion)
  - By De Morgan :

    ~(Premise 1 ∧ ... ∧ Premise n) ∨ Conclusion
  - By the definition of → :

    Premise 1 ∧ ... ∧ Premise n → Conclusion

Proof by Contradiction: Example 1

- Theorem:

  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 1

- Theorem:
  Not every CPSC 121 student got an above average grade on midterm 1.
- Proof:
  - Assume that every CPSC 121 student got an above average grade on midterm1
  - Let $g_1, g_2, \ldots, g_n$ be the grades of the students. And let a be the exam average
  - Then $g_i > a$ for $1 \leq i \leq n$
  - And $g_1 + g_2 + \ldots + g_n > n*a$
    or $(g_1 + g_2 + \ldots + g_n) / n > a$
  - But $(g_1 + g_2 + \ldots + g_n) / n$ IS the average and is equal to a.
  - Contradiction.
  - Therefore, Not every 121 students got an above average grade on midterm1. QED

Proof by Contradiction: Example 2

- A rational number can be expressed as a/b for some $a \in Z$, $b \in Z^+$ with no common factor except 1.
- Theorem: *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!

Proof by Contradiction: Example 2

- Theorem: *For all real numbers x and y, if x is a rational number, and y is an irrational number, then x+y is irrational.*
- Proof
  - Assume x is a rational number, y is an irrational number and that x+y is a rational number.
  - Then $x+y = a / b$ for some $a \in Z$ and some $b \in Z^+$
  - Since x is rational, $x = c / d$ for some $c \in Z$ and some $d \in Z^+$
  - Then $(c / d) + y = a / b$
  - and $y = (a / b) - (c / d) = (ab - bc) / bd$
  - Since $ab - bc$ and bd are integers and $bd > 0$, y is rational.
  - This is a contradiction. Therefore the original theorem is true. QED

Proof Strategies

- So Far:

$\forall x \in D, P(x)$.	let x be an arbitrary ….
$\exists x \in D, P(x)$.	with a witness
$p \rightarrow q$	by assuming the LHS or prove the contrapositive
assume ~p and derive F	proof by contradiction

- We can use all the propositional logic strategies. Each inference rule suggests a strategy:

$p \wedge q$	by proving each part
$p \vee q$	by proving either part
$p \vee q$	by assuming ~p and showing q (same strategy as for $p \rightarrow q$!!)

and so on.

How should you tackle a proof?

- Have lots of strategies on hand, and switch strategies when you get stuck:
- Try using WLOG, exhaustion, or witness approaches to strip the quantifiers
- Try antecedent assumption on conditionals
- Try the contrapositive of conditionals
- Try contradiction on the whole statement or as part of other strategies

How should you tackle a proof? (cont')

- Work forward, playing around with what you can prove from the premises
- Work backward, considering what you'd need to reach the conclusion
- Play with the form of both premises and conclusions using logical equivalences
- Finally, disproving something is just proving its negation

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