Introduction to Computers and Programming

Prof. I. K. Lundqvist

Lecture 20
May 5 2004

Proof by Truth Table

- Proposition
  $x \rightarrow y$ and $(\neg x) \vee y$ are logically equivalent

x	y	$x \rightarrow y$	$\neg x$	$(\neg x) \vee y$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	1	0	1

Definitions

- **Even**
  An integer n is even, iff $n=2k$ for some integer k.
  – n is even $\leftrightarrow \exists$ an integer k such that $n = 2k$

- **Odd**
  An integer n is odd, iff $n=2k+1$ for some integer k.
  – n is odd $\leftrightarrow \exists$ an integer k such that $n = 2k+1$

- **Divisible**
  An integer n is divisible by m, iff n and m are integers such that that there is an integer k such that $mk=n$
  – n is divisible by m $\leftrightarrow \exists$ an integer k such that $mk=n$

The sum of two even integers is even

1. Rewrite as a condition (using if, then)
2. Write the hypothesis (beginning) and the conclusion (end)
   1. For beginning: establish notation and unwind definitions
   2. For end: unwind definitions backwards
3. ... and ... wait ...

The sum of two even integers is even

Proof:

1. If x and y are even integers, then x+y is even [conditional]
2. Let x and y be integers [hypothesis]
3. x is even, so 2|x [def. of even]
4. There is an integer, e.g., a, with x=2a [def. of divisible]
5. y is even, so 2|y [likewise for y]
6. There is an integer, e.g., b, with y=2b [as above]
7. (x+y)=2(a+b) so take c = (a+b) [add equations in 4 and 6]
8. There is an integer, e.g, c, with (x+y)=2c [def. of divisible]
9. (x+y) is even, so 2|(x+y) [def. of even]
10. x + y is even [conclusion]

Direct Proof

- Show that a given statement is true by simple combination of existing theorems
  - With or without mathematical manipulations
- Template for Proof of an if-then theorem
  - First sentence(s) of proof is the hypothesis restated
  - Last sentence(s) of proof is the conclusion of the theorem
  - Unwind the definitions, working from both end and beginning of the proof
  - Try to forge a ‘link’ between the two halves of your argument.

Direct Proof Example (1/2)

Given:

1. JaneB is in Course_16 or in Course_6
2. If JaneB does not like Unified, she is not in Course_16
3. If JaneB likes Unified, she is smart
4. JaneB is not in Course_6

Prove that JaneB is smart

Direct Proof Example (2/2)

1. $C\_16 \vee C\_6$	Given
2. $\neg U \rightarrow \neg C\_16$	Given
3. $U \rightarrow S$	Given
4. $\neg C\_6$	Given

5. C_16 [1,4 Disjunctive Syllogism]
6. U [2,5 Modus Tollens]
7. S [3,6 Modus Ponens]

Concept Question

Given $p \rightarrow q$;   What is $\neg q \rightarrow \neg p$?

1. Negation
2. Implication
3. Contrapositive
4. I don't know

Proof of Implication

- Direct proof of $p \rightarrow q$
  - the **contrapositive**, $\neg q \rightarrow \neg p$, is **logically equivalent** to $p \rightarrow q$
  - We can **prove** $\neg q \rightarrow \neg p$ via the **direct approach** and then the original implication, $p \rightarrow q$, is proven.
- Indirect proof
  - **first assume that q is false**. Then use rules of inference, logical equivalences, and previously proved theorems to **show that p must also be false**

Note that it may not be the case that q is false. If q is true then the implication holds. We assume that q is false so that we can explore this scenario and show that p must necessarily be false as well.

Ex: Give an indirect proof of "If 3n + 2 is odd, then n is odd."

Recall again that this statement is implicitly a universal quantification "$\forall n(3n + 2 \text{ is odd} \rightarrow n \text{ is odd})$."

Proof: We will prove the **contrapositive**, "If n is not odd, then 3n + 2 is not odd. That is, "If n is even, then 3n + 2 is even."

[step 1: Write assumptions] Let n be an even integer.

[step 2: Translate assumptions into a form we can work with]

Then $n = 2k$ for some integer k. [Definition of even]

[step 3: Work with it until it is in a form we need for concl.]

So $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$.

[step 4: Realize that you're there and state your conclusion.]

So $3n + 2 = 2{*}m$ where $m = (3k + 1)$, so $3n + 2$ is even.

Indirect Proofs

$p \rightarrow q \equiv \neg q \rightarrow \neg p$ (the contrapositive)

- Prove the implication $p \rightarrow q$:
  - Assume $\neg q$,
  - Show that $\neg p$ follows

Prove: "if $a + b \geq 15$, then $a \geq 8$ or $b \geq 8$". Where a, b are integers

$$(a + b \geq 15) \rightarrow (a \geq 8) \vee (b \geq 8)$$

- Assume: $(a < 8) \wedge (b < 8)$
- Proof: $\Rightarrow (a \leq 7) \wedge (b \leq 7)$

  $\Rightarrow (a + b) \leq 14$

  $\Rightarrow \mathbf{(a + b) < 15}$

Ex: Prove that **if n is an integer and n^2 is odd, then n is odd**.

Direct Approach: Let **n be an integer such that n^2 is odd**. Then (by the definition of odd), **$n^2 = 2k + 1$ for some integer k**. Now we want to know something about n (namely that *n is odd*). It is difficult to go from *information about n^2 to information about n*. It is much easier to go in the other direction. Let's try an indirect approach.

Indirect Approach: The original statement is $\forall n \in Z(n^2 \text{ is odd} \rightarrow n \text{ is odd})$. So the **contrapositive** is $\forall n \in Z(n \text{ is not odd} \rightarrow n^2 \text{ is not odd})$. Recalling that a number is not odd iff the number is even, we have: $\forall n \in Z(n \text{ is even} \rightarrow n^2 \text{ is even})$.

Let **n be an even integer**. Then (by the definition of even), **$n = 2k$** for some integer k. So **$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$**. Now $2k^2$ is an integer since k is and so we have expressed n^2 as 2(some integer). So by the definition of even, **n^2 is even**.

Proof by Contradiction

Theorem: $\sqrt{2}$ is an irrational number

Assume $\sqrt{2}$ is a rational number
Then $\sqrt{2} = a/b$ | a, b: relatively prime integers, and $b \neq 0$

$\rightarrow 2 = a^2/b^2$

$\rightarrow 2b^2 = a^2$

$\rightarrow a^2$ is even, $\therefore$ a is even, $a=2k$ for some k

$\rightarrow 2b^2 = (2k)^2 = 4k^2$

$\rightarrow b^2 = 2k^2$

a, b are no longer relatively prime

$\rightarrow b^2$ is even, $\therefore$ b is even, $b=2j$ for some j

Proof by Contradiction

- Assume, along with the hypotheses, the **logical negation** of the result we wish to prove, and then reach some kind of contradiction.
- To prove: "If P, then Q"
  - assume P and $\neg$Q.
  - the contradiction we arrive at could be some conclusion contradicting one of the assumptions
    (or something obviously untrue like 1 = 0)

Proof by Contradiction Example

Rainy days make gardens grow.
Gardens don't grow if it is not hot.
When it is cold outside, it rains.

1. $R \rightarrow G$
2. $\neg H \rightarrow \neg G$
3. $\neg H \rightarrow R$

- Prove that it is hot

4. $\neg$H	**[Assumption]**
5. R	[Modus Ponens 3,4]
6. G	[Modus Ponens 1,5]
7. $\neg$G	[Modus Ponens 2,4]

6,7 = **Contradiction!**

[Example]

Prove " if 5n+6 is odd, then n is odd" by contradiction

Proof: Assume 5n+6 is odd and n is even

- Then n = 2k for some integer k
- 5n+6 = 5* 2k + 6 = 2 * (5k + 3)
- Since 5k+3 is an integer, 5n+6 is an even number, contradicting the assumption that it was odd
- Thus if 5n+6 is odd, then n is odd

Proof by Induction

A proof by Induction has five basic parts:

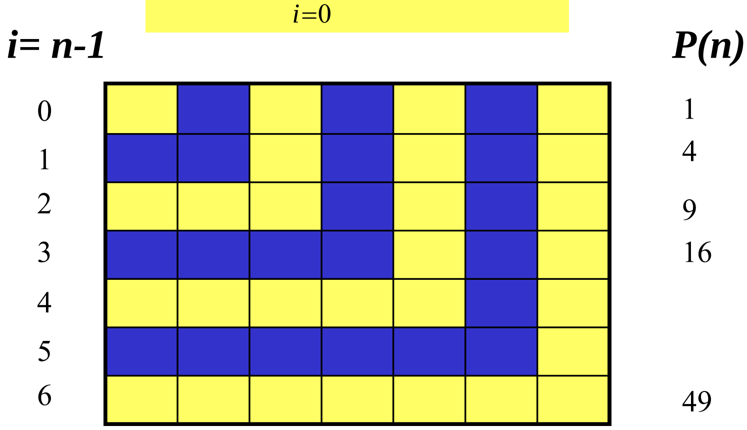
1. State the proposition
2. Verify the base case
3. Formulate the inductive hypothesis
4. Prove the inductive step
5. State the conclusion of the proof

Proof by Induction

Prove $\forall n \geq 0\ P(n)$, where

$P(n)$ = "The sum of the first n positive odd integers is n^2"

$$P(n) = \sum_{i=0}^{n-1} (2i+1) = n^2$$



Proof by Induction

- **Basis Step**: Show that the statement holds for the smallest case (n = 0)

$$\sum_{i=0}^{-1} (2i+1) = 0 = 0^2$$

- **Induction Step**: Show that if statement holds for n, then statement holds for $n+1$.

$$\sum_{i=0}^{n} (2i+1) = \sum_{i=0}^{n-1} (2i+1) + [2n+1]$$

$$= n^2 + [2n+1]$$

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

Proof by Induction

Factorial(n) is the product of the first n positive integers

- **Basis Step**:

  F(0) = 1

- **Induction Step**:

Assume: F(n-1) = (n-1)*(n-2)*…*2*1

multiply both sides by n,

n*F(n-1) = n*(n-1)*…*3*2*1

= F(n)

Rule of Inference	Tautology	Name
p $\therefore p \lor q$	$p \to (p \lor q)$	Addition
$p \land q$ $\therefore p$	$(p \land q) \to p$	Simplification
p, q $\therefore p \land q$	$(p \land q) \to p \land q$	Conjunction
$p, p \to q$ $\therefore q$	$(p \land (p \to q)) \to q$	Modus Ponens
$\neg q, p \to q$ $\therefore \neg p$	$(\neg q \land (p \to q)) \to \neg p$	Modus Tollens
$p \to q, q \to r$ $\therefore p \to r$	$((p \to q) \land (q \to r))$ $\to (p \to r)$	Hypothetical Syllogism
$p \lor q, \neg p$ $\therefore q$	$((p \lor q) \land \neg p) \to q$	Disjunctive Syllogism
$p \lor q, \neg p \lor r$ $\therefore q \lor r$	$(p \lor q) \land (\neg p \lor r)$ $\to q \lor r$	Resolution