CISC-102
Fall 2016
Week 11

Logical Consequence and Arguments

Consider the expression:

p is true and p implies q is true , as a consequence we can deduce that q must be true.

This is a logical argument, and can be written symbolically as,

$p, p \rightarrow q \vdash q$

where: $p, p \rightarrow q$ is called a sequence of ***premises***, and q is called the ***conclusion***.
The symbol $\vdash$ denotes a logical consequence.

A sequence of premises whose logical consequence leads to a conclusion is called an ***argument***.

Valid Argument

We can now formally define what is meant by a valid argument.

> **The argument $P_1, P_2, P_3, \ldots, P_n \vdash Q$ is valid if and only if $P_1 \wedge P_2 \wedge P_3 \wedge \ldots \wedge P_n \rightarrow Q$ is a tautology.**

Example: Consider the argument

$$p \rightarrow q, q \rightarrow r, \vdash p \rightarrow r$$

We can see if this argument is valid by using truth tables to show that the proposition:

$$(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$$

a tautology, that is, the proposition is true for all T/F values of p,q,r.

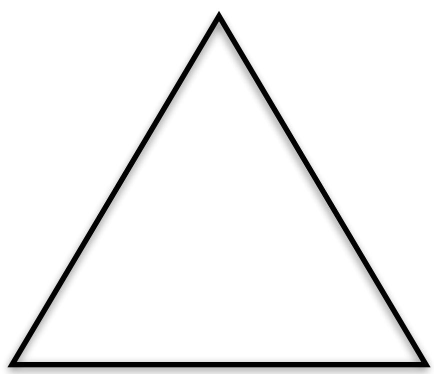
p	q	r	$(p \rightarrow q) \wedge (q \rightarrow r)$	$(p \rightarrow r)$	$(p \rightarrow q) \wedge (q \rightarrow r), \rightarrow (p \rightarrow r)$
T	T	T	T	T	T
T	T	F	F	F	T
T	F	T	F	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	T	F	F	T	T
F	F	T	T	T	T
F	F	F	T	T	T

Consider the following argument:

If two sides of a triangle are equal **then** the opposite angles are equal
T is a triangle with two sides that are not equal

The opposite angles of T are not equal

(With this notation the horizontal line separates a sequence of propositions from a conclusion.)



Let p be the proposition
"two sides of a triangle are equal"
and let q be the proposition
"the opposite angles are equal"

We can re-write the argument in symbols as:

$$p \to q, \neg p \vdash \neg q$$

and as the expression:

$$[(p \to q) \wedge \neg p] \to \neg q$$

We can check whether this is a valid argument by using a truth table, and verifying that the expression is a tautology.

p	**q**	$[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$
T	T	
T	F	
F	T	
F	F	

Propositional Functions

Let P(x) be a propositional function that is either true or false for each x in A.

That is, the domain of P(x) is a set A, and the range is {true, false}. NOTE: Sometimes propositional function are called *predicates*.

Observe that the set A can be partitioned into two subsets:

- Elements with an image that is true.
- Elements with an image that is false.

In particular we may define the *truth set* of P(x) as:
$T_P = \{ x : x \text{ in } A, P(x) \text{ is true}\}$

Examples: Consider the following propositional functions defined on the positive integers.

P(x): $x + 2 > 7$; $T_P = \{x : x > 5\}$
P(x): $x + 5 < 3$; $T_P = \varnothing$
P(x): $x + 5 > 1$; $T_P = \mathbb{N}$

Quantifiers
There are two widely used logical quantifiers

Definition:
Universal Quantifier: $\forall$ (for all)

Let P(x) be a propositional function. A quantified proposition using the propositional function can be stated as:

$(\forall x \in A)\ P(x)$ (for all x in A P(x) is true)

$T_p = \{x : x \in A, P(x)\} = A$

Or if the elements of A can be enumerated as:

$A = \{x_1, x_2, x_3, \ldots\}$

We would have:

$P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge \ldots$ is true.

Definition:
Existential Quantifier: $\exists$(there exists)

Let P(x) be a propositional function. A quantified proposition using the propositional function can be stated as:

$(\exists x \in A)\ P(x)$ (There exists an x in A *s.t.* P(x) is true)

$T_P = \{x : x \in A, P(x)\} \neq \emptyset$

Or if the elements of A can be enumerated as:

$A = \{x_1, x_2, x_3, \ldots\}$

We would have:

$P(x_1) \vee P(x_2) \vee P(x_3) \vee \ldots$ is true.

Quantifiers

Statement	True when:	False when:
$(\forall x \in A)\ P(x)$	$P(x)$ is true for every $x \in A$.	$P(x)$ is false for one or more $x \in A$.
$(\exists x \in A)\ P(x)$	$P(x)$ is true for one or more $x \in A$.	$P(x)$ is false for every $x \in A$.

Propositional functions with more than one variable

Consider the following illustrative example:

Let $p(x,y)$ be the proposition that "$x+y = 10$" where the ordered pair $(x,y) \in \{1, 2, ..., 9\} \times \{1, 2, ..., 9\}$.

Consider the following quantified statements:

1. $\forall x \exists y \; p(x,y)$
2. $\exists y \forall x \; p(x,y)$

1. Says: "for every x there exists a y such that $x + y = 10$"
2. Says: "there exists a y such that for every x, $x+y = 10$"

Statement 1. is true, and statement 2, is false by inspection. This simply illustrates that the concepts that we have seen can be extended to more that one variable.

Methods of Proof

Axioms

Definition: An *axiom* is a statement or proposition that is regarded as being established, accepted, or self-evidently true.

Mathematics is a system created by humans, and can be developed in its entirety by a small collection of axioms that are assumed to be true.

Euclid of Alexandria (300 BC) developed an axiomatic approach for geometry starting with only 5 axioms.

In this course we have been making quite a few assumptions about what we accept as true. In practice it would be excruciating to prove everything from basic principles. There is an estimate that proving 2+2=4 from basic principles requires more than 20,000 steps.

Logical Deduction

We use logical deduction in a natural way to solve puzzles of many different forms, ranging from playing Sudoku to solving murder mystery's.

In mathematics logical deduction is used as we proceed from step to step in a proof.

The basic rule that we use, as described in formal logic, is:

$p, p \rightarrow q \vdash q$

We can verify that this is a valid argument. We can also reason this out informally as:

If p is true, and p implies that q is true, then we may conclude that q is true.

As an aside, this *inference rule* is named "*modus ponens*" by logicians, and is also known as the "law of detachment". You can look this up if you are interested but as far as this course goes, I think the informal explanation is sufficient.

Methods of Proof

Proof by Induction

Verifying closed form expressions for recursively defined functions and summations is a perfect use for mathematical induction.

The Fibonacci function

Fib(0) = 0
Fib(1) = 1
Fib(n) = F(n-1) + F(n-2) for all Natural numbers $n \geq 2$.

NOTE: (Some variants start the function with Fib(1) = 1, and Fib(2) =1.)

The first few Fibonnaci numbers are
Fib(0) = 0, Fib(1) = 1, Fib(2) = 1,
Fib(3) = 2, Fib(4) = 3, Fib(5) = 5,
Fib(6) = 8, Fib(7) = 13, Fib(8) = 21,
Fib(9) =34.

The Fibonacci sequence is named after Fibonacci. His real name was Leonardo Pisano Bogollo, and he lived between 1170 and 1250 in Italy."Fibonacci" was his nickname, which roughly means "Son of Bonacci". As well as being famous for the Fibonacci Sequence, he helped spread through Europe the use of Hindu-Arabic Numerals (like our present number system 0,1,2,3,4,5,6,7,8,9) to replace Roman Numerals (I, II, III, IV, V, ...).

We can prove that the sum of squares of the first n Fibonacci numbers is:

$$\sum_{i=0}^{n} F_i^2 = F_n \cdot F_{n+1}$$

Proof:
Base: $F_0^2 = 0^2 = F_0 \cdot F_1$.
Induction Hypothesis: Assume $\sum_{i=0}^{k-1} F_i^2 = F_{k-1} \cdot F_k$, for $k \geq 1$.
Induction Step:

$$\begin{aligned}
\sum_{i=0}^{k} F_i^2 &= F_k^2 + \sum_{i=0}^{k-1} F_i^2 \\
&= F_k^2 + F_{k-1} \cdot F_k \\
&= F_k(F_k + F_{k-1}) \\
&= F_k \cdot F_{k+1}
\end{aligned}$$

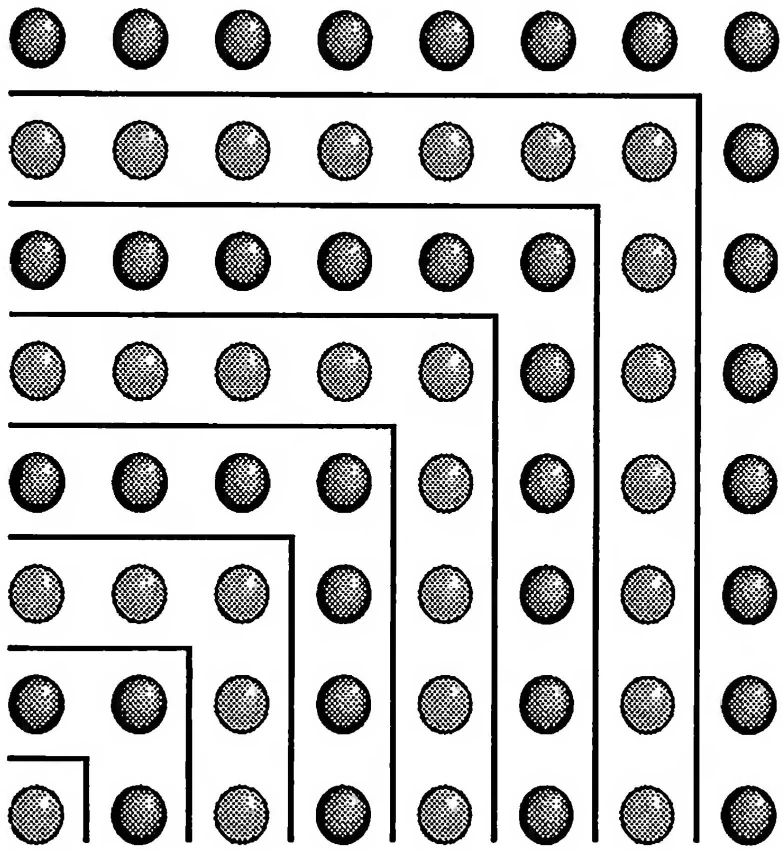
And the following question about the sum of odd numbers is easily proved using induction.

$$1 + 3 + \cdots + (2n - 1) = \sum_{i=1}^{n} 2i - 1 = n^2$$

Proof:
Base: $1 = 1^2$
Induction Hypothesis: Assume that $\sum_{i=1}^{k} 2i - 1 = k^2$.
Induction Step:

$$\begin{aligned} \sum_{i=1}^{k+1} 2i - 1 &= \sum_{i=1}^{k} (2i - 1) + 2k + 1 \\ &= k^2 + 2k + 1 \\ &= (k+1)(k+1) \\ &= (k+1)^2 \end{aligned}$$

Here is a proof by “picture” of the sum odd integers.



Strong Induction

Let b denote a base case values for the induction and let P(n) denote the proposition to prove.

Strong induction or the 2nd form of induction is the same technique as the 1st form of induction except:

- In the 1st form of induction the hypothesis is stated as:
  Assume P(k) is true for $k \geq b$
- In the 2nd form of induction the hypothesis is stated as:
  Assume P(b), P(b+1), ..., P(k-1), P(k) is true.

or alternately

Assume P(i) is true, for i such that $b \leq i \leq k$.

We may need to use more that one base case to "bootstrap" the induction process.

Consider the recursively defined integer sequence:

$a_0=1$, $a_1=2$, $a_2=3$ and $a_n=a_{n-1}+a_{n-2}+a_{n-3}$ for all $n \geq 3$, $n \in \mathbb{N}$

Let P(n) be the proposition $a_n \leq 3^n$.

Prove P(n) is true for all $n \in \mathbb{N}$.

Proof: (strong induction)

Base: $a_0 = 1 = 3^0 \leq 3^0$, $a_1=2 \leq 3^1$, $a_2 = 3 \leq 3^2$.

Induction Hypothesis: Assume that P(1), P(2), …, P(k) are true.

Induction Step: Show P(1), P(2), …, P(k) are true, implies P(k+1) is true.

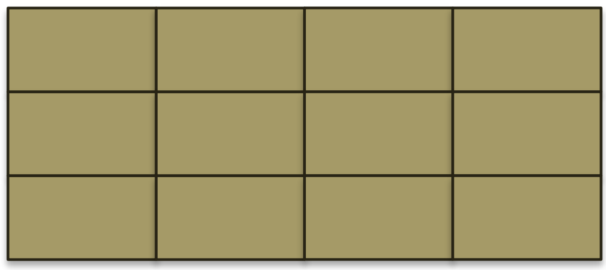
$a_{k+1} = a_k + a_{k-1} + a_{k-2}$ (definition)

$\leq 3^k + 3^{k-1} + 3^{k-2}$ (induction assumption)

$< 3(3^k)$ ($3^{k-1} < 3^k$, and $3^{k-2} < 3^k$, for $k \geq 1$)

$= 3^{k+1}$ □

Consider a chocolate bar consisting of n rectangular pieces. You may break the bar (or part of a bar) with a single horizontal or vertical cut that splits the bar into two rectangles. How many breaks are needed to break the bar into n individual pieces?



Suppose the bar has one piece, that is n = 1. Then 0 breaks are needed. Suppose the bar has 2 pieces, then 1 break is needed. What about 3 or 4 pieces?

Let P(n) be the proposition that an n piece rectangular chocolate bar (as described) can be split into n individual pieces using n-1 breaks.

Proof: (Strong induction)
Base: n = 1, 0 breaks.
Induction Hypothesis: P(1), P(2), …, P(k) are true.
Induction Step: Show that P(1), P(2), …, P(k) are true implies that P(k+1) is true.

Consider a rectangular bar with k+1 pieces. Use 1 break to get two rectangular bars, of i and j pieces such that i+j = k+1.

By the induction hypothesis the bar with i pieces can be split with i-1 breaks, and the bar with j pieces can be split with j-1 breaks. Putting this together we need:

$$i-1 + j-1 + 1 \text{ breaks}$$

to split the bar with k+1 pieces. Observe that

$$i-1+j-1+1 = i+j-1=k+1-1,$$

which is the required result. □

Proof Templates

Prove that $2 \mid a(a+1)$, for all $a \in \mathbb{N}$.

An informal proof of this result could be the observation that either a or (a+1) must be divisible by 2, and therefore the product a(a+1) must also be divisible by 2.

However, in our studies we saw a very similar example that provides a “template” for proving the result.

That is: Let $a \in \mathbb{N}$ show that $3 \mid a(a+1)(a+2)$, that is the product of three consecutive integers is divisible by 3.

Familiar facts from high school math, as well as results that we have seen this term and used <u>repeatedly</u> can be assumed without further proof.

In practice for a course like this there is usually a very similar proof that you have seen that can be used as a template. And this will implicitly use assumptions that you may use.

Proof by cases.

Proofs by cases can be used for the following results:

1. Prove that $2 \mid a(a+1)$, for all $a \in \mathbb{N}$.

2. Prove that $3 \mid a(a+1)(a+2)$, for all $a \in \mathbb{N}$.

The basic template is to partition all possible outcomes into individual cases that are easier to handle separately than together.

Consider the following problem:

Prove that $6 \mid a(a+1)(a+2)$, for all $a \in \mathbb{N}$.

Proof: We can use case analysis from the previous two results (result 1, result 2) as a template. We already know by result 2 that:

$3 \mid a$, or $3 \mid a+1$ or $3 \mid a+2$ so.

Case 1. $3 \mid a$, then by result 1. $2 \mid (a+1)(a+2)$. Thus $6 \mid a(a+1)(a+2)$.

Case 2. $3 \mid a+2$, then by result 1. $2 \mid a(a+1)$. Thus $6 \mid a(a+1)(a+2)$.

Case 3. $3 \mid a+1$.

Case 3.1 a and a+2 are both even, then $2 \mid a$ and $3 \mid a+1$, so $6 \mid a(a+1)(a+2)$.

Case 3.2 a and a+2 are both odd, therefore a+1 is even, so $2 \mid a+1$, so a+1 is divisible by 2 and 3 and we are back to square 1. OOPS!

Prove that $6 \mid a(a+1)(a+2)$, for all $a \in \mathbb{N}$.

Here is a very slick proof:

Proof: Observe that $a(a+1)(a+2) = (a+2)!/(a-1)!$ which is equal to:

$$6\binom{a+2}{3} = 6\frac{(a+2)!}{3!(a-1)!}$$

We know that $\binom{a+2}{3}$ is an integer so we conclude that:
$6 \mid a(a+1)(a+2)$. □

Prove that a(a+1)(a+2)(a+3) is divisible by 24.

Let's try the previous solution as a template.

Proof: Observe that a(a+1)(a+2)(a+3) = (a+3)!/(a-1)! which is equal to:

$$24\binom{a+3}{4} = \frac{24(a+3)!}{4!(a-1)!}$$

We know that $\binom{a+3}{4}$ is an integer so we conclude that:
24 | a(a+1)(a+2)(a+3). □

Theorem: Every collection of 6 people includes 3 people who have all met each other, or 3 people who have never met.

Proof:
Let x denote one of the 6 people. Now consider the number of people from the other 5 who have met or have not met x.

There are two cases to consider.

- case 1: There are 3 or more people who have met x.
    - case 1.1 Among those who have met x, none have met each other, so this satisfies the requirements of the theorem.
    - case 1.2 Among those who have met x, at least one pair have met each other. Since they have also met x, this satisfies the requirements of the theorem

- case 2: There are 3 or more people who have not met x.
    - case 2.1 Those who have not met x, have all met each other, and this satisfies the requirements of the theorem.
    - case 2.2 Amongst those who have not met x, there are 2 (or more) who have not met each other. That pair together with x satisfy the requirements of the theorem.

Thus we have proved that every collection of 6 people includes 3 people who all have met each other, or 3 people who have never met by using an exhaustive case analysis. □

Note: This collection of 6 people can be thought of as a set of 6 elements. People either have met or have never met, there is no other possibility. In general the “met” property could be any arbitrary (Boolean) function of two elements of the set that returns true or false.

Direct Proof:

Let a be a natural number. If a is even then a+1 is odd and a+2 is even.

Proof: If a is an even natural number we have

$a = 2m$ for some natural number m.

then

$a + 1 = 2m + 1$ implying that a is odd,

and

$a+2 = 2m + 2 = 2(m+1)$ implying that a is even. □

Indirect Proof

If a is an integer and a^2 is odd then a is also odd.

Proof: If a^2 is odd we have:

$$a^2 = 2m + 1$$

Now a can be written as:

$$a = \sqrt{2m+1}$$

and I don't know how to continue this proof.

Sometimes the contrapositive leads to a simpler proof.

The proposition is:

If a is an integer and a^2 odd **then** a is also odd.

or for a an integer: a^2 odd $\rightarrow$ a odd

The contrapositive would be

not a odd $\rightarrow$ not a^2 odd or

a even $\rightarrow$ a^2 even.

If a is an integer and a^2 is odd then a is also odd.

Proof: We will prove that the contrapositive is true. That is, let a be an integer, if a is even then a^2 is even.

We know in general that if $b \mid c$ then $b \mid mc$ for any integer m. Therefore as a special case we have $2 \mid a$ so $2 \mid a^2$. Therefore we can conclude that if a^2 is odd then a must also be odd. □

An *indirect proof* proves the contrapositive of the proposition.

Proof by Contradiction.
Let a be an integer, if a^2 is even then a is even.

How would we prove this proposition?

Proof: Suppose a^2 is even and a is odd. If a is odd then we have the equation: $a = 2m + 1$, where m is an integer. Now square both sides to get the equation:

$$a^2 = 4\,m^2 + 4m + 1. \qquad (1)$$

Let $n = m^2 + m$, and notice that n is an integer. Thus equation (1) simplifies to:

$$a^2 = 4\,n + 1$$

and is odd. Assuming a^2 is even and a odd leads to a contradiction, so we conclude that if a^2 is even then a is even. □

Proof by the Pigeon Hole principle:

Prove that at least 5 days of the month of March fall on the same week day.

Proof: Imagine that there are 7 pigeon holes with 4 chairs inside each. There are 31 days in March so at most 28 days can be seated on the chairs. Therefore there are at least 5 days that fall on the same day of the week. □

The pigeon hole principle is a particular case of a larger method of proof called proof by contradiction.

Proof by Contradiction

We know that p, $p \rightarrow q \vdash q$ that is if p is true and $p \rightarrow q$ is true then the logical consequence is that q must be true.

Suppose we know that a proposition is false, and we want to prove that p is true. Consider this round about method of proving that p is true.

$\neg p, \ \neg p \rightarrow F \vdash p$

We can verify this with a truth table.

p	$\neg p$	$\neg p \rightarrow F$	$\neg p \wedge \neg p \rightarrow F \rightarrow p$
T	F	T	T
F	T	F	T

Prove that at least 5 days of the month of March fall on the same week day.

Let p be the proposition that 5 or more days of the month of March fall on the same day of the week. Now $\neg p$ is the proposition that at most 4 days of the month of March fall on the same day of the week. The false proposition is $7 \times 4 \geq 31$. ($7 \times 4 \geq 31$ is the same as saying that every day in March gets to sit in a chair in the pigeon holes.) The assumption that at most 4 days of March fall on the same day of the week leads to a contradiction. □

Prove that $\sqrt{2}$ is irrational.

Proof: We show that the assumption that $\sqrt{2}$ is rational leads to a contradiction.

If $\sqrt{2}$ is rational then we can write it as the quotient a/b where a,b are both integers. Furthermore, we assume that a/b have no common factors, that is we reduced the quotient to lowest terms. Thus:

$$\sqrt{2} = a/b$$

square both sides of equation:

$$2 = a^2/b^2$$

now multiply both sides by b^2:

$$2\,b^2 = a^2.$$

Therefore a^2 is even implying a is even.
If a is even we can write it as $a = 2m$ for some integer m. Now we get

$$2b^2 = 4m^2.$$

Divide both sides by 2:

$$b^2 = 2m^2.$$

So b^2 is even implying b is even.

We have established that both a and b are even, but when we started we said that a and b have no common factors. Thus we have established a contradiction to the assertion that $\sqrt{2}$ is rational, so we conclude that $\sqrt{2}$ is irrational. □

Recall we saw a proof by contradiction when we studied prime factorization. (Week 5)

Theorem: Every integer $n > 1$ is either prime or can be written as a product of primes.

Proof:

(1) Suppose there is an integer $k > 1$ that is the largest integer that is the product of primes. This then implies that the integer $k+1$ is not prime or a product of primes.

(2) If $k+1$ is not prime it must be composite and:

$$k+1 = ab, \;\; a,b \in \mathbb{Z}, \;\; a,b \notin \{1,-1, k+1, -(k+1)\}.$$

(3) Therefore, $|a| < k+1$ and $|b| < k+1$.
So $|a|$ and $|b|$ are prime or a product of primes.

(4) Since $k+1$ is a product of a and b it follows that it too is a product of primes.

(5) Thus we have contradicted the assumption that there is a largest integer that is the product of primes, and we can therefore conclude that every integer $n > 1$ is either prime or written as a product of primes.

In proving that "every integer $n > 1$ is either prime or can be written as a product of primes" we used the well ordering principle to justify the fact that if there is an integer that is the product of primes then there is a least integer that is the product of primes. Well ordering is also implied when we argue that we can express a rational number in lowest terms.

Some additional problems.

1. Prove $|xy| = |x|\,|y|$ for all integers x and y.
(case analysis)

2. Prove that the sum of two rational numbers is rational. (direct proof)

3. Prove that if $3n+2$ is odd, then n is odd.
(proof by contradiction)