MATH 135 - Algebra for Honours Math

Kevin Carruthers

Winter 2013

Implications

Definition: An impication is a statement S such that a hypothesis (or assumption) H ensures the validity of the conclusion C, and may either be true or false. An implication is only false if a hypothesis is true and the conclusion is false (ie a counter-example exists). In other words, for S: $P \implies Q$ (P implies Q), S is true unless P is true and Q is false.

Note that this can give confusing results such as

- If $1 = 2$, then $2 = 2$
- If $1 = 2$, then $2 = 3$

Because $1 = 2$ is a false hypothesis, both of these implications are true, regardless of the vailidty of their conclusion.

Direct Proof

For a direct proof, we start by assuming the hypothesis, and derive the conclusion.

Proposition: ***For*** $S_0 = A \implies B$***,*** $S_1 = B \implies C$***, and*** $S_2 = A \implies C$***, prove*** S_2 ***given*** S_0 ***and*** S_1***.***

Proof:
Assume A. Since both A and $A \implies B$ are true, B is true. Since B and $B \implies C$ are true, C is true. Thus $A \implies C$ is true. QED.

Proposition: ***Given*** S_0***,*** S_1***, and*** S_2***, assume*** S_0 ***and*** S_2 ***are true. Must*** S_1 ***be true?***

Proof:
$B \implies C$ is false if and only if B is true and C is false. If C is false, we have A is false, so we have both $A \implies B$ and $A \implies C$ are true, but $B \implies C$ is false. Thus S_0 and S_2 do not imply S_1. QED.

Divisibility

Definition: An integer m divides an integer n if there exists an integer k such that $n = km$. This is denoted as $m \,|\, n$.

Proposition: *Transitivity of Divisibility*
Let a, b, and c be integers. If $a \,|\, b$ and $b \,|\, c$, then $a \,|\, c$.

Proof:
Since $a \,|\, b$, there exists an integer k such that $b = ka$.
Since $b \,|\, c$, there exists an integer j such that $c = jb$.
Then $c = jka$. Since $jk \in \mathbb{Z}$, we have $a \,|\, c$. QED.

Things to Remember

1. Always assume the hypothesis is true.
2. Never assume the conclusion is true.
3. Starting from the hypothesis, think of what can be derived using definitions, theorems, and logical deductions.
4. Look toward the conclusion, think of what needs to be achieved to prove the conclusion.

Sets

A set is a collection of objects. We use the notation $e \in S$ for element e in set S. Sets can not have duplicate elements and may be defined in any order. They may be described in **set builder notation** $S = \{x_0, x_1, ..., x_n\}$, $T = \{2k + 1 \bigm| k \in \mathbb{R}\}$

If S and T are sets, the **cartesian product** of S and T is

$$S \times T = \{(a, b) \bigm| a \in S, b \in T\}$$

The order of elements within each pair does matter.

For a finite set S, the **cordinality** of S is the number of elements in S, denoted $\bigl|S\bigr|$. Note that $\bigl|S \times T\bigr| = \bigl|S\bigr|\bigl|T\bigr|$. The empty set is the only one with a cordinality of 0.

Operations

Note that we use $\wedge$, $\vee$, and $\neg$ to denote "and", "or", and "not".

1. Union: $S \cup T = \{x \bigm| x \in S \vee x \in T\}$
2. Intersection: $S \cap T = \{x \bigm| x \in S \wedge x \in T\}$

3. Complement: $S^c = \{x \mid x \notin T\}$. Note that $S^{c^c} = S$.
    - Complements are transitive, ie $(A \cap B)^c = A^c \cap B^c$.
4. Difference (relative complement of B in A): $S \setminus T = \{x \mid x \in S \land x \notin T\}$. In other words, $S \setminus T = S \cap B^c$.
    - Relative complements are inversely transitive, ie $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$.

Subsets

Definition: S is a **subset** of T ($S \subseteq T$) if and only if for every $x \in \mathbb{R}$, $x \in S \implies x \in T$. Note that $S \subseteq S$ and the zero set is a subset of every other set.

For a set S, the **power set** is the set of all possible subsets of S, denoted by $\mathcal{P}(S)$ or 2^S

Example: for $S = \{1, 2\}$, $\mathcal{P}(S) = \big\{\{\}, \{1\}, \{2\}, \{1, 2\}\big\}$ thus $\{2\} \in \mathcal{P}(S)$ but $2 \notin \mathcal{P}(S)$ so $\big\{\{2\}\big\} \subseteq \mathcal{P}(S)$. $\big|\mathcal{P}(S)\big| = 4$, or $\big|\mathcal{P}(n)\big| = 2^{\left|n\right|}$

Equality

$A = B$ if and only if for every $x \in \mathbb{R}$, $(x \in A \iff x \in B)$. From the definitions of a subset, we also have $A = B \iff A \subseteq B$ and $B \subseteq A$.

Proposition: $S \cap (T \cup U) = (S \cap T) \cup (S \cap U)$

> *Proof:*
> Let $x \in S \cap (T \cup U)$.
> So $x \in S$ and $x \in T \cup U$.
> We have two cases:
> If $x \in T$, $x \in S \cap T$.
> If $x \in U$, $x \in S \cap U$.
> Therefore, $x \in (S \cap T) \cup (S \cap U)$. QED.

Quantifiers

The **universal quantifier** $\forall$ means "for all" and the **existential quantifier** $\exists$ means "there exists".

Examples:

$\forall x$, $x = 3$ is false if $x \in \mathbb{Z}$ but true if $x \in \{3\}$

$\exists y$, $y < 1$ is true if $y \in \mathbb{Z}$ but not if $y \in \mathbb{N}$

We can thus compare these qualifiers to logical statements. For example

$$\forall x, P(x) = P(x_0) \wedge P(x_1) \wedge P(x_2) ...$$

and

$$\exists x, P(x) = P(x_0) \vee P(x_1) \vee P(x_2) ...$$

Proving Statements Containing Quantifiers

Note that some quantifiers can be hidden in words. For example, the mathematical definition of divisibility is $a \,|\, c \implies \exists k \in \mathbb{Z} \bigm| c = ka$

1. To prove that something exists, construct this thing.
2. To prove a universal property, select an arbitrary member of the universe and prove the property for this instance.

Nested Qualifiers

Proposition: $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} \bigm| y < x$

Proof:
Let $x \in \mathbb{R}$,
Then $y = x - 1$ satisfies $y \in \mathbb{R}$ and $y < x$. QED.

but **Proposition:** $\exists y \in \mathbb{R}, \forall x \in \mathbb{R} \bigm| y < x$

Proof:
If such a y exists, then $x = y$ does not satisfy $y < x$.
This is a contradiction, thus the proposition is false. QED.

Proposition: $\forall x \in \mathcal{P}(\mathbb{N}), x \notin \{\} \implies \exists y \in x, \forall z \in x \bigm| y < z$

Proof:
Can be accepted logically. QED.

Binary Relations

Let X be a set. A **binary relation** on X is a two-variable predicate $\mathcal{R}$ defined on X (ie for $\{(x, y) \in X \text{ x } X\}, \mathcal{R}(x, y)$ may be either true or false). When $\mathcal{R}(x, y)$ holds, we say *x is $\mathcal{R}$ -related to y* and write $x\mathcal{R}y$.

Equality, ordering, and divisibility are all examples of relations. We also have

$$A \subseteq B \iff \forall x \in S, (x \in A \implies x \in B)$$

and for any $A, B \in \mathcal{P}(S)$ the disjointedness relation

$$A \perp B \iff A \cap B = \{\}$$

For a binary relation on set X, the relation is

- Reflexive if $\forall x \in X, x\mathcal{R}x$
- Symmetric if $\forall x, y \in X, x\mathcal{R}y \implies y\mathcal{R}x$
- Transitive if $\forall x, y, x \in X, x\mathcal{R}y \wedge y\mathcal{R}z \implies x\mathcal{R}z$

Equivalence Relations

Let X be a non-empty set. An **equivalence relation** on X is a binary relation on X that is reflexive, symmetric, and transitive. The most common example of this is for $S = \{(x, y) \in \mathbb{R} \text{ x } \mathbb{R} \mid x = y\}, x\mathcal{R}y$ is an equivalent relation.

Implication Modifiers

Converses

The **converse** of $A \implies B$ is $B \implies A$. Note that the converse does not necessarily have the same truth value as the original implication. If both statements are true, then the elements within them are equivalent.

Negations

Let A, B, and C be statements. Then

1. $\neg(A \wedge B) \iff (\neg A) \vee (\neg B)$
2. $\neg(A \vee B) \iff (\neg A) \wedge (\neg b)$
3. $\neg(A \implies B) \iff A \wedge \neg B$
4. $\neg(\neg A)) \iff A$

Let S be a set, $P(x)$ is a statement dependant on $x \in S$. Then

1. $\neg(\forall x \in S, P(x)) \iff \exists x \in S, \neg P(x))$
2. $\neg(\exists x \in S, P(x)) \iff \forall x \in S, \neg P(x))$

To find the negation of $P(x)$, we can do the following

$$\begin{aligned}
P(x) &= \exists y \ \in \ \mathbb{R}, \forall x \ \in \ \mathbb{R} \bigm| y < x \\
\neg P(x) &= \neg(\exists y \ \in \ \mathbb{R}, \forall x \ \in \ \mathbb{R} \bigm| y < x) \\
&= \forall y \ \in \ \mathbb{R}, (\neg(\forall x \ \in \ \mathbb{R} \bigm| y < x)) \\
&= \forall y \ \in \ \mathbb{R}, \exists x \ \in \ \mathbb{R} \bigm| y \geq x
\end{aligned}$$

Contrapositive

Definition: The contrapositive of $P \implies Q$ is $\neg Q \implies \neg P$. A statement and its contrapositive are equivalent, and it can sometimes be easier to prove the contrapositive.

Proposition: ***For $n \ \in \ \mathbb{Z}$, if n^2 is even then n is even***

Proof:
Suppose n is odd.
Then $n = 2k + 1$ for some $k \ \in \ \mathbb{Z}$.
So $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$.
Then n^2 is odd. Thus we have n is odd $\implies$ n^2 is odd, so n^2 is even $\implies$ n is even.
QED.

Use a contrapositive when the hypothesis does not give much to work with or when the negation of the implication is nicer.

Contradiction

Assume the conclusion is false (ie the contrapositive is false). If you derive something impossible, the assumption must be wrong.

Deduction Overview

Methods of deduction:

- Direct: assume the hypothesis and find the conclusion.
- Example: especially with quantifiers, find an example which breaks the implication.
- Contrapositive: prove the contrapositive.
- Absurdity: Assume the implication (or contrapositive) is false, try to find something blatantly contradictory.

Induction

Induction is useful when proving general statements $\forall x$.

Principle of Mathematical Induction

Suppose $P(n)$ is a statement for $n \geq n_0$. If

1. $P(n_0)$ is true, and
2. $\forall k \geq n_0, P(k) \implies P(k+1)$.

Then, by induction, $P(n)$ is true $\forall n \geq n_0$.

Weak Induction

Weak induction is a general technique based directly on the Principle of Mathematical Induction (henceforth refered to as POMI), and is suited to proving statements of the form "$\forall n \geq n_0, P(n)$". It consists of two steps:

1. the **base case** (prove $P(n_0)$), and
2. the **induction step** (chose an arbitrary $k \geq n_0$ for which we assume $P(k)$, then prove $P(k+1)$).

Then we simply invoke the POMI to conclude $\forall n, P(n)$.

Proposition: $\forall n \geq 2, (1+x)^n > 1 + nx$

Proof:
For $n = 2$ we have

$$\begin{aligned} P(2) &= (1+x)^2 \\ &= 1 + 2x + x^2 \\ &> 1 + 2x + 0 \\ &> 1 + 2x \end{aligned}$$

This proves $P(2)$
Assume that $(1+x)^k > 1 + kx$. Then

$$\begin{aligned} P(k+1) &= (1+x)^{k+1} \\ &= (1+x)^k(1+x) \\ &> (1+kx)(1+x) \\ &> 1 + kx + x + kx^2 \\ &> 1 + (k+1)x + 0 \\ &> 1 + (k+1)x \end{aligned}$$

So $\forall k \geq 2, P(k) \implies P(k+1)$. Thus, by POMI, $\forall n \geq 2, (1+x)^n > 1 + nx$. QED.

Strong Induction

Strong induction is an alternative to weak induction which may be used when $P(k+1)$ is dependant on either multiple past cases or a single past case $P(j)$ where the relative location of $j < k$ cannot be determined.

Principle of Strong Induction, v1

Definition: Let $P(n)$ be a property concerning integers $n \geq n_0$. Suppose that the following are true:

1. $P(n_0)$, and
2. $\forall k \geq n_0, \forall n_o \leq j \leq k, P(j) \implies P(k+1)$

Then $\forall n, P(n)$.

Proposition: ***Every natural number*** $n > 1$ ***can be expressed as a product of primes***

Proof:
For any $n \geq 2$, if n is prime then n is the product of a single prime (itself). Thus n is prime $\implies P(n)$.
Assume n is composite. By definition $\exists m \bigm| 1 < m < n \wedge m \,|\, n$.
For $n = md, d \in \mathbb{N}$, we have $1 < d < n$.
By induction hypothesis, $P(m) \wedge P(d)$, which means we can express m and d as products of primes. The we can write

$$m = p_0 p_1 ... p_s$$

and

$$d = q_0 q_1 ... q_t$$

so

$$n = md = (p_0 p_1 ... p_s)(q_0 q_1 ... q_t)$$

is a product of primes. By POSI, $\forall n \geq 2, n$ is a product of primes. QED.

Principle of Strong Induction, v2

The first version of POSI can fail given certain low values of k (for certain $P(n)$ we may have $P(n) \iff n \geq b \wedge b \geq n_0$). We thus modify POSI to seperately verify the multiple base cases of $P(j)$ for $n_o \leq j \leq b$.

Definition: Let $P(n)$ be a property concerning integers $n \geq n_0$. Suppose, for some integer $b \geq n_0$, the following are true:

1. $P(n_0), P(n_0 + 1), ..., P(b)$, and
2. $\forall k \geq b, \forall n_o \leq j \leq k, P(j)$

Proposition: $\forall n \geq 60, n = 7x + 11y; n, x, y \in \mathbb{Z}, x, y \geq 0$. ***Use the following equalities:***

$$1 = 7(-3) + 11(2) \tag{1}$$
$$1 = 7(8) + 11(-5) \tag{2}$$
$$60 = 7(7) + 11(1) \tag{3}$$

Proof:
Equation (3) clearly verifies $P(60)$.
Since we have x is multiplied by 7 and $7 < 11$, we take $P(j)$ with $60 \leq j \leq 66$ as the base cases, all of which can be verified with a list of equations (omitted).
Assume that $k \geq 67$ is such that $P(j)$ holds for all $60 \leq j < k$.
Since $k \geq 67, k - 7 \geq 60$ and so $P(k-7)$ is true, thus

$$k - 7 = 7x + 11y$$

for some x and y. We can manipulate this equation to have

$$k = 7(x+1) + 11y$$

and since $x + 1 \; \in \; \mathbb{Z} \wedge x + 1 \geq 0, P(k)$.
Thus we have shown that whenever $k \geq 67, P(60), ...P(k-1)$ all true imply $P(k)$. By POSI, this proposition is true. QED.