MA-138

Haria

October 2025

1 Lecture 1 - Sets

1.1 What are Sets

Definition 1. *A set is a collection of elements*

Commonly these are denoted by a listing of elements within braces. For example $\{1, 2, 3\}$ is the set containing 1, 2, and 3. Sometimes ellipses may be used inside the set

Example 1. $\{0, 1, 2, 3, \dots\}$ *denotes the set of the natural numbers* $\mathbb{N}$

When ellipses are seen a natural continuation of elements is assumed in this case the rest of the natural numbers. Note here $\mathbb{N}$ contains 0.

Definition 2. *If x is and element of a set X we nay write $x \in X$*

Example 2. $1 \in \mathbb{N}$

We can also demonstrate the converse

Example 3. $-1 \notin \mathbb{N}$

1.2 Set Relations

1.2.1 Equality

The first thing we want to be able to tell about pairs of sets is whether two are the same.

Definition 3. *Sets X and Y are equal if for every $x \in X$ we have $x \in Y$ and for every $y \in Y$ we have $y \in X$*

From this definition falls out two interesting things

- Sets do not care about the order of their elements
- Sets do not care how many times their elements occur

This makes them fundamentally different from lists.

Example 4. $\{1, 2, 3\} = \{2, 2, 3, 1, 1, 3, 3\}$

1.2.2 Empty Set

Before the next relation it is useful to introduce a special set known as the empty set.

Definition 4. *There exists a set $\emptyset$ such that there does not exist an $x \in \emptyset$ called the empty set*

An interesting result is given two empty sets $\emptyset_1$ and $\emptyset_2$ these two are always equal. This is because any element in the first is necessarily in the second and vice versa as their are no elements in either. This tells us that there is only one empty set.

1.2.3 Numeric Sets

Another useful set to know is as follows before the next relation

Definition 5. *The set denoted* $[n] = \{0, 1, 2, \ldots n - 1\}$

This is the set of all the natural numbers less than n and is non-standard notation.

1.2.4 Subsets

Definition 6. *We can say a set X is a subset of a set Y if for every $x \in X$ we also know that $x \in Y$ this is denoted $X \subseteq Y$*

Example 5. $\{0, 1\} \subseteq \{0, 1, 2\}$

Example 6. $[n] \subseteq [n + 1]$

From here we can derive the fact that if $X \subseteq Y$ and $Y \subseteq X$ we can say $X = Y$. Each direction of the subset satisfies half the condition for equality so having both directions of the subset we can claim equality. this is similar to how when $x \leq y$ and $y \leq x$ we know that $x = y$.

For every set X we can also say two things

1. $\emptyset \subseteq X$
2. $X \subseteq X$

Which is also similar to what we can say for $\leq$

1.3 Set Function

1.4 Power Set

Every set can have many power sets so it is useful to be able to easily reference this collection of subsets

Definition 7. *For a set X let $\mathcal{P}(X)$ denote its power set such that $x \in \mathcal{P}(X)$ if and only if $x \subseteq X$*

Example 7. $\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$

Example 8. $\mathcal{P}(\emptyset) = \{\emptyset\}$

It is important to remember that $\{\emptyset\}$ is a distinct set from $\emptyset$ as the first contains $\emptyset$ as an element $\emptyset \in \{\emptyset\}$ We also have a useful result that

$$|\mathbb{P}([[n]])| = 2^n$$

As for each element in $[[n]]$ for each subset of $[[n]]$ it can either be in or out of the subset.

2 Lecture 2 + 3 - Functions

2.1 Specification

Definition 8. ***Specification*** *: Let X be a set and $S(x)$ be a property for $x \in X$. We can form a set*

$$\{x \in X | S(X)\}$$

This gives the subset of X satisfying $S(x)$ for all x in the subset

An example of this is $\{k \in \mathbb{N} | k < n\}$ being the set of natural numbers less than n. This is the same as the set $[[n]]$ as defined earlier.

It is important to make sure you keep track of what set you are specifying against. For example the sets $\{k \in \mathbb{N} | x^2 - 1 = 0\}$ and $\{k \in \mathbb{Z} | x^2 - 1 = 0\}$ are different sets as the latter also contains -1. Its also important to remember you are taking a subset of a set in this invocation. Not doing so is unrestricted comprehension and leads to Russel's paradox.

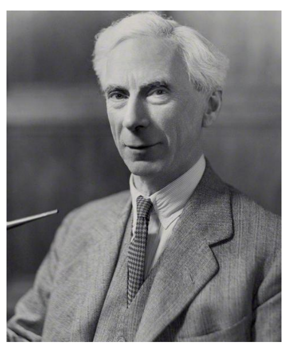

Figure 1: Russel angered by your use of unrestricted comprehension

2.2 Functions

2.2.1 Basics

Here we can start with a slightly informal definition of a function.

Definition 9. *Let X and Y be sets. A function f from X to Y (denoted $f : X \to Y$) contains three pieces of information*

1. *A domain X*
2. *A codomain Y*
3. *A rule mapping every in $x \in X$ to one $f(x) \in Y$*

Two examples of functions are given as $f_1 : \mathbb{N} \to \mathbb{N}$ with $f_1(x) = x^2$ and another example is $f_2 : \mathbb{N} \to \mathbb{Z}$ with $f_2(x) = x^2$. These both are are different functions as they have different codomains. Two functions are only equal if all three pieces of information agree.
It is important to note that the rule portion of a function need not be given by a formula and can instead just tell you where each element goes. For example $g : \{0, 1\} \to \{2, 3\}$ can have its rule expressed as $g(0) = 2$ and $g(1) = 2$. We can also get the useful property

$$|[[n]] \to [[m]]| = m^n$$

If a function f is $X \to X$ we say it is a function on X. A special function is the identity function on X $id_X : X \to X$ given by rule $id_X(x) = x$

2.2.2 Types of functions

Definition 10. *A function $f : X \to Y$ is called injective if $f(x) = f(x') \Rightarrow x = x'$ for all $x, x' \in X$*

Definition 11. *A function $f : X \to Y$ is called surjective if for any $y \in Y$ there is an $x \in X$ such that $y = f(x)$*

And if a function satisfies both of these we can call it bijective.
For finite sets we can say a lot of things about injections and surjections between them. For a pair of sets X, Y if $|X| = |Y|$ then any injective function is surjective. this is due to the fact to be injective each element in the domain needs a separate element in the codomain. So their are as many elements in the image as the domain which is the same as the size of the codomain so every element in the codomain is hit. And for the reverse argument each element in the codomain binds a unique element in the domain which is every element in the domain. It cant bind 2 elements to one element in the codomain otherwise the image would not be the codomain and as such would not be surjective.
We also get the fact we have no injections $f : [[n]] \to [[m]]$ if $m < n$ and no surjections $f : [[n]] \to [[m]]$ if $n < m$

2.2.3 Cardinality

Definition 12. *Given any sets X and Y, X and Y have the same cardinality iff there exists a bijection $f : X \to Y$. This is denoted $|X| = |Y|$*

Definition 13. *For a finite set X if there is a bijection $f : [[n]] \to X$ then we may say that $|X| = n$*

This makes sense for finite sets but has some interesting implications for infinite sets. Consider and $f : \mathbb{Z} \to \mathbb{N}$ defined as follows

$$f(x) = \begin{cases} 2x & \text{if } x \geq 0 \\ -2x - 1 & \text{if } x < 0 \end{cases}$$

This function is a bijection between the two sets mapping even naturals to positives and odds to negatives. As such we have $|\mathbb{N}| = |\mathbb{Z}|$ despite $\mathbb{N} \subseteq \mathbb{Z}$. We can construct a similar argument between $\mathbb{N}$ and $\mathbb{Q}$ by use of **The Cantor Pairing Function** which constructs the bijection between pairs of natural numbers and naturals which gets you 99% of the way to a bijection and infact shows that $|\mathbb{N}| \geq |\mathbb{Q}|$ as there are multiple pairs of naturals that can give a single rational number.
This is however not possible between $\mathbb{R}$ and $\mathbb{N}$. It can be shown there is no such bijection. this is done using Cantor's diagonalization argument to prove that there is no surjection.

Proof. Assume that theres is a surjection $f : \mathbb{N} \to \mathbb{R}$ This would allow us to list elements of $\mathbb{R}$ on the output. Here we will represent elements of $\mathbb{R}$ in binary expansions

$$\begin{aligned} f(1) &= 0.010110101111\ldots \\ f(2) &= 0.101100110001\ldots \\ f(\cdots) &= \cdots \end{aligned}$$

Now we con construct a new number x. We make x by making the nth digit of x the opposite of the nth digit of $f(n)$. Now the question is : is x on our list. If x is in the image of f then there is some k such that $f(k) = x$ but this means that x will differ from $f(k)$ in the kth digit so x cannot be $f(k)$ so x cannot be in the image so f cannot be a surjection □

We can also very similarly consider cantor theorem

Proposition 1. *There is no surjection $X \to \mathcal{P}(X)$*

Proof. By contradiction assume there is a function $f : X \to \mathcal{P}(X)$ such that f is a surjection. The means for an $A \in \mathcal{P}(X)$ we know there is an $a \in X$ so that $f(a) = A$ We can define a set $C \subseteq X$ as follows

$$C = \{x \in X | x \notin f(x)\} \in \mathcal{P}(X)$$

As f is a surjection there exists a d such that $f(d) = C$. We can consider two cases.

1. Consider $d \in C$. this gives that $d \in f(d)$ so by defninition $d \notin f(d)$ leading to a contraditcion
2. Consider $d \notin C$ this gives that $d \notin f(d)$ so by definition $d \in C$ leading to a contradiciotn

Both paths lead to a contradition so we can assume our premise was wrong meaning that there is no such surjection. □

This is somewhat related to how russels pradox works.

3 Lecture 4 + 5 + 6- More sets

3.1 Products

Definition 14. *Given $x \in X, y \in Y$ We can construct an ordered pair (x, y). We may say for two pairs $(x, y) = (x', y')$ if and only if $x = x', y = y'$*

Definition 15. *The cartesian product $X \times Y$ is the set of all pairs (x, y) such that $X \in X, y \in Y$*

$$X \times Y = \{(x, y)|x \in X, y \in Y\}$$

We can from here get a few algebraic properties of the cartesian product.

Proposition 2. $X \times \emptyset = \emptyset$

Proof. Suppose by contradiction $X \times \emptyset \neq \emptyset$. this means there is a pair $(a, b) \in X \times \emptyset$ this means there is a $b \in \emptyset$ which is false yeilding a contradiction. □

We also know that $|[[m]] \times [[n]]| = mn$ and that $X \times Y$ does not generally equal $Y \times X$.

Definition 16. $X^2 = X \times X$

3.2 Relations

Definition 17. *A relation R from $X \to Y$ consists of three parts*

1. *A set X as the domain*
2. *A set Y as the codomain*
3. *A set $R \subseteq X \times Y$*

You may write xRy to say that x is related to y is $(x, y) \in R$

Definition 18. *A relation R from $X \to Y$ may be called graphical if the every $x \in X$ there is only one pair $(x, y) \in R$*

3.2.1 Functions

Definition 19. *A function $f : X \to Y$ is a graphical relation F from $X \to Y$ such that*

$$f(x) = y \Leftrightarrow (x, y) \in F$$

Example 9. *1. $\{(0,1),(1,2),(2,3)\} \subseteq [[3]] \times [[5]]$ is a graphical relation and associates to $f(x) = x + 1$*

2. $\{(0,0),(0,1)\} \subseteq [[1]] \times [[2]]$ is not graphical as there is more than one pair for zero

Definition 20. *A function f with graphical relation F can be called injective if for every $y \in Y$ there is at nmost one $(x, y) \in F$*

3.3 Unions

Definition 21. *Given two sets X, Y we can define their union as the set*

$$\{z | z \in X \text{ or } z \in Y\}$$

And given a set of sets $\mathbb{X}$

$$\bigcup_{X \in \mathbb{X}} X = \{x | x \in X \text{ for some } X \in \mathbb{X}\}$$

For example let $\mathbb{X} = \{[[n]] | n \in \mathbb{N}\}$ then $\bigcup_{X \in \mathbb{X}} X = \mathbb{N}$

3.4 Intersections

Definition 22. *The intersection of two sets X, Y is*

$$X \cap Y = \{z | z \in X \text{ and } z \in Y\}$$

Let $\mathbb{X}$ be a set of sets

$$\bigcap_{x \in \mathbb{X}} X = \{z | z \in X \text{ for all } X \in \mathbb{X}\}$$

For example let $\mathbb{X} = \{[[n]] | n \in \mathbb{N}\}$ then $\bigcap_{X \in \mathbb{X}} X = \emptyset$

3.5 Set difference

Definition 23. *The set difference of X, Y is*

$$X - Y = \{x \in X | x \notin Y\}$$

For example $\mathbb{Z} - \mathbb{N} = \mathbb{Z}_{>0}$

3.6 Alegebra of Sets

3.6.1 Difference

The following identities hold for the set difference

- $X - \emptyset = X$
- $\emptyset - X = \emptyset$
- $X - X = \emptyset$

3.6.2 Union

The union is associative and commutative. The following identities also hold

- $X \subseteq X \cup Y$
- $X \cup \emptyset = X$

3.6.3 Intersection

The intersection is also associative and commutative. The following idnetities also hold

- $X \cap Y \subseteq X$
- $X \cap \emptyset = \emptyset$

3.6.4 Misc

Both the intersection and the union can distrobute over each other. The following identity also holds.

$$X - (Y \cup Z) = (X - Y) \cap (X - Z)$$

The identity also holds if you reverse the unions and intersections

4 Lecture 6 - Composition

Definition 24. *Suppose $f : X \to Y$ and $g : Y \to Z$ are both functions then we can compose these to get the new function $(g \circ f) : X \to Z$ where $(g \circ f)(x) = g(f(x))$*

The associated graphical realtionship is as follows

$$\{(x, g(f(x)))|x \in X\} \subseteq X \times Z$$

Theorem. $(f \circ g) \circ h = f \circ (g \circ h)$

Definition 25. *Given an $f : X \to Y$ we can say a function $g : Y \to X$ is a*

- *left inverse of f if $(g \circ f) = id_X$*
- *right inverse of f if $(f \circ g) = id_Y$*

Theorem. *Given $f : X \to Y$ we can say*

- *If f has a left inverse it is injective*
- *If f has a right inverse it is surjective*

5 Lecture 7 - Relations

5.1 Functions on Functions

Definition 26. *Given a function $f : X \to Y$ we say show the image of $A \subseteq X$ as*

$$f(A) = \{f(x) \in Y | x \in A\} \subseteq Y$$

Definition 27. *Given a function $f : X \to Y$ we may say the preimage of a set $B \subseteq Y$ as follows*

$$f^{-1}(B) = \{x \in X | f(x) \in B\} \subseteq X$$

5.2 Relations - Equivalence Properties

Definition 28. *Suppose we have a set X and a relation $R \subseteq X^2$ we may make the following comments on the relation*

- *If for all $x \in X$ we know that xRx we may call this relation reflexive*
- *If for all $x, y \in X$ we have $xRy \implies yRx$ we may call this relation symmetric*
- *If for all $x, y, z \in X$ we have $xRy \wedge yRz \implies xRz$*

Definition 29. *If a relation $R \subseteq X^2$ is all of reflexive symmetric and transitive we may call this an equivalence relation.*

The idea of an equivalence relation is to capture the idea of what makes two things equal. If there are properties that you dont care about for an object you can create an equality relation. Though not an equvalence relation (due to there being no set of sets) we can somewhat see this idea in the definition of equality for sets where we ingore ordering and repetion for the determination of equality.

5.3 Partial Orders

Definition 30. *Suppose X is a set and a realtion $R \subseteq X^2$. We may call this relation antisymetric if for all $x, y \in X$, xRy and yRx implies that $x = y$*

An example of such a relation is $\geq$

Definition 31. *Suppose we have a set X and a relation $R \subseteq X^2$ that is reflexive transitive and antisymetric. We may call this realtion a partial order and we may call the pair (X, R) a poset.*

Example 10. *A special poset is the boolean poset on X which is the pair $(\mathcal{P}(X), \subseteq)$*

5.4 Total Orders

Definition 32. *Suppose we have a set X and a relation $R \subseteq X^2$ if we have that for all $x, y \in X$ that either xRy or yRx we may call this relation total.*

Definition 33. *If a relation R is total and is a partial order we may call it a total order.*

6 Lecture 8

6.1 Partitions

Definition 34. *Suppose X is a set. A set $P \subseteq \mathcal{P}(X)$ is a partition if*

- *Every element of P is non-empty*
- $\bigcup_{p \in P} p = X$
- *Elements of P are mutually disjoint*

We can note two sepcial partitions one that partitions the set ontp singletons and one that contiains only one partition that is the entire set itself.

6.2 Equivalence Classes

Definition 35. *Suppose we have a set X with an equivalence relation $E \subseteq X^2$. Given an $x \in X$ we may show its equivalence class as follows*

$$[x]_E = \{y \in X | xEy\}$$

Similar to the two partitions given eralier we have the identity relation whos equivalence classes are singletons and the universal relation whose sole equivalence class is the whole set X.

We may denote the set of all equvalence classes as follows

$$X/E = \{[x]_E | x \in X\}$$

We can also define a function $q_E : X \to X/E$ defined as $q_E(x) = [x]_E$

Proposition 3. *Given a set X and an eqivalence relation E we may say X/E is a partition of X*

Proof. To prove this we must go through each of the properties of partitions

- As we know that $x \in [x]_E$ we can see no class is enmpty
- By the point above we know that all x is in at least one class so the union is the original set
- We will attempt to prove by contradiction that all classes are dissjoint. Suppose by contradiciotn for some some x, y that there is a $z \in [x]_E \cap [y]_E$ where $[x]_E \neq [y]_E$. We can deduce that xRz and yRz. By the properties of an equivalence relation we can deduce xRy. This means for all $y' \in [y]_E$ we can say $y' \in [x]_E$ and also show the same for x so they are the same set leading to a contradiction.

□

6.3 Well definedness

Functions out of equicvalence classes have to be careful tnhat they operate thae same no matter what representation of a class it operates on. So if we have some $x \neq y, [x]_E = [y]_E$ we do want to have $f([x]_E) = f([y]_E)$. As susch we can introduce a property called well definedness.

Definition 36. *Consider two sets X, Y an equivalence relation on X,E and a funciton $f : X \to Y$. We may call f well defined if for all $x, x' \in X$ if xEx' then $f(x) = f(x')$*

This definition can be used to the induce a function $f_E : X/E \to Y$.

7 Lecture 9

Omiited because tedius to write

8 Lecture 10 - Modular Arithmetic

Definition 37. *LEt E_n be the equivalence relation on $\mathbb{Z}$ fegiven by*

$$xE_ny \iff y = x + kn$$

$$[a]_n = \{x \in \mathbb{Z} | aE_nx\}$$

Is the congruence class of a module n

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{[a]_n | a \in \mathbb{Z}\}$$

Given a congruence class $[b]_n$ we say b is a representative instance for $[b]_n$

Theorem. *There is a bijection $q_n : [[n]] \to \frac{\mathbb{Z}}{n\mathbb{Z}}$ that takes a natural number to an equivalence class. To do the inverse case we must choose a representative for the class.*

$$q_n(k) = [k]_n$$

Definition 38. *Recall $[b]_n = [b + kn]_n, k \in \mathbb{Z}$.*

If $[x]_n = [y]_n$ we write

$$x \equiv y \mod n$$

and say x is congruent to y modulo n

Definition 39. *We define the following operations*

- *Addition : $[a]_n + [b]_n := [a + b]_n$*
- *Multiplication : $[a]_n \times [b]_n := [a \times n]_n$*
- *Negation : $-[a]_n := [-a]_n$*

We also define two special elements

- *$[0]_n$ is the zero element so $[0]_n + a = a$ and $[0]_n \times b = [0]_n$*
- *$[1]_n$ is the unit(identity??) element so $[1]_n \times b = b$*

With these definitions we want to have that if $a \equiv c \mod n$ and $b \equiv d \mod n$ then $[a + b]_n = [c + d]_n$. This is the same as saying we want addition to be a function $+ : \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}} \to \frac{\mathbb{Z}}{n\mathbb{Z}}$. So we are essentially looking for a well definedness.

Proof. The fact $[a]_n = [c]_n$ means that $c = a + kn$. Like wise for b, d we can say $d = b + jn$.

$$\begin{aligned} [c + d]_n &= [a + kn + b + jn] \\ &= [a + b + (k + j)n] \\ &= [a + b]_n \end{aligned}$$

□

We may carry out similar proofs for multiplication and negation

Proof. The fact $[a]_n = [c]_n$ means that $c = a + kn$. Like wise for b, d we can say $d = b + jn$.

$$\begin{aligned} [c \times d]_n &= [(a + kn)(b + jn)]_n \\ &= [a \times b + akn + bkn + jkn^2]_n \\ &= [a \times n + (ak + bk + jkn)n]_n \\ &= [a \times b]_n \end{aligned}$$

□

Proof. The fact $[a]_n = [c]_n$ means that $c = a + kn$.

$$-[a]_n = [-1]_n \times [a]_n$$

By the fact multiplication is well defined negation is well defined $\square$

By the fact that all of these definitions are in terms of simple aritmetic theorems regarding these arithmetic operations still hold under modular arithmatic so we get to keep commutivity associativy distributivity which is very fun :3.

Example 11. *Say you where told to find the last didgit of* 3^{1000}*. This is athe same as finding an* $x \in [[10]]$ *such that* $x \equiv 3^{1000} \mod 10$

$$3^{1000} = 9^{500} \equiv (-1)^{500} = 1 \mod 10$$

9 Lecture 11 - Boolean Operators

Definition 40. *A Boolean is an element of the set* $\{T, F\}$

Consider the statement "2 is a prime number". This statement has an boolean value in this case that value is T. Another statement is "2 is an odd number" this aslo has a boolean value which in this case is T. Both of these statements are propositions.

Definition 41. *A proposition is a statement that evaluates to a boolean*

Definition 42. *A boolean operator* σ *of arity n (an n-ary function) is a function* $\sigma : \{T, F\}^n \to \{T, F\}$

Definition 43. *Negation :* $\neg : \{T, F\} \to \{T, F\}$*. This has arity 1*

p	$\neg p$
T	F
F	T

Definition 44. *Or :* $\vee : \{T, F\}^2 \to \{T, F\}$ *is a 2-ary operator defined as follows*

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Definition 45. *And :* $\wedge : \{T, F\}^2 \to \{T, F\}$ *is a 2-ary operator defined as follows*

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Definition 46. *Implies :* $\Rightarrow: \{T,F\}^2 \to \{T,F\}$ *is a 2-ary operator defined as follows*

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Definition 47. *Is equivalent to (iff) :* $\Leftrightarrow \{T,F\}^2 \to \{T,F\}$ *is a 2-ary operator defined as follows*

p	q	$p \Leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Definition 48. *We say two* n*-ary boolean operators are equal if they are equal as funtions.*

Example 12. *The expression* $\neg((\neg P) \vee (\neg Q)) = P \wedge Q$

Theorem. *Any boolean operator is a composition of those operators given above (not even all five is needed as some can be expressed as other. all operators can be made with (nand)/(or with negation))*

10 Lecture 12

The operations given last time (and, or) satosfy identities similarly to intersections and unions.

For the or we have

- $P \vee T = T$
- $P \wedge F = P$

It is also commutative and associative. We also know that $P \vee P = P$

For and we know

- $P \wedge T = P$
- $P \wedge F = F$

They are also commutative and associative and $P \wedge P = P$

These also distrobute over each other

- $P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee Q)$
- $P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge Q)$

They also realte bye demorgans law **PUT DM LAW**

Definition 49. *A boolean operator* $f : \{T, F\}^n \to \{T, F\}$ *is a tautology if* $f(x) = T$ *for all* $x \in \{T, F\}^n$

Definition 50. *A boolean operator* $f : \{T, F\}^n \to \{T, F\}$ *if* $f(x) = F$ *is an antimony for all* $x \in \{T, F\}^n$

Example 13. *The statement* $P \vee \neg P$ *is a tautology*

Definition 51. *The lookup table for a boolean operations* $f : \{T, F\}^n \to \{T, F\}$ *is a two columned table. The first column is* $x \in \{T, F\}^n$ *and the second is* $f(x)$

For large and complex tables this can be hard to do (well not hard but very fucking long)

Example 14.

$$(P \wedge (Q \vee R)) \Rightarrow R$$

P	Q	R	f
F	F	F	T
F	F	T	T
F	T	F	T
F	T	T	T
T	F	F	T
T	F	T	T
T	T	F	F
T	T	T	T

Theorem. *If* f, g *are of the same aritty then* $f = g$ *if and only if* $f \Leftrightarrow g$

The following are useful tautologies

- DNE : $\neg\neg P \Leftrightarrow P$
- Contraposition : $(Q \Rightarrow P) \Leftrightarrow (\neg P \Rightarrow \neg Q)$
- Bidirectionality : $(P \Leftrightarrow Q) \Leftrightarrow ((P \Rightarrow Q) \vee (Q \Rightarrow P))$
- LEM : $(P \vee \neg P)$
- Modus Ponens : $(P \wedge (P \Rightarrow R)) \Rightarrow R$
- Chaining : $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$
- Contradiction : $((\neg P) \Rightarrow F) \Rightarrow P$

11 Lecture 14

Theorem. *Suppose* $X \neq \emptyset$

$$\forall x \forall y P(x, y) \Leftrightarrow \forall y \forall x P(x, y)$$

We can also firther show the one way chain of implications

$$\begin{aligned}\forall x \forall y P(x,y) &\Rightarrow \exists x \forall y P(x,y)\\ &\Rightarrow \forall y \exists x P(x,y)\\ &\Rightarrow \exists x \exists y P(x,y)\end{aligned}$$

And further

$$\exists x \exists y P(x,y) \Leftrightarrow \exists y \exists x P(x,y)$$

Theorem. *Suppose $X = \emptyset$*

$$\forall x P(x) \Leftrightarrow T$$

$$\exists x P(x) \Leftrightarrow F$$

Definition 52. *Let A be a set of axioms. Let D be a set of deduction rules. A proof of S from A is a sequence of statements $(S_k)_{k=0}^n$ such that S_k is either an axiom or S_k can be deduced from $(S_i)_{i<k}$ using elements of D.*

Example 15.

$$A = \{(\exists X, |X| = 0), (\exists X, |X| = n \Rightarrow \exists Y, |Y| = 2^n)\}$$

$$D = \{(P \wedge (P \Rightarrow Q)) \Rightarrow Q\}$$

Theorem.

$$\exists x, |x| = 2$$

Proof.

$$\begin{aligned}&S_0 : (\exists X, |X| = 0)\\ &S_1 : (\exists X, |X| = 0 \Rightarrow \exists Y, |Y| = 1)\\ &S_2 : \exists Y, |Y| = 1 \text{ by } D\\ &S_3 : (\exists Y, |Y| = 1 \Rightarrow \exists Z, |Z| = 2)\\ &S_4 : \exists Z, |Z| = 2 \text{ by } D\end{aligned}$$

□

PRoving tings like this is unweildy so we generally use the following definition

Definition 53. *Proof (Informal) : A convincing argument of a statement.*

Theorem. *There are arbitrariliy large rpimes*

$$\forall n \in \mathbb{N} \exists p \in \mathbb{N}, (p > n) \wedge (prime(p))$$

The normal proof for this is done and it is done by contradiction. Proofs done be contradiction is done by $(\neg P \Rightarrow F) \Rightarrow P$ Which under the assumption of LEM is a tautology. One part of the proof entails the fact a;; primes $p \leq n$ where from there you construct a set of such primes. This relies on the axiom of specification and when doing formal proof you would need to quote this and do it poperly but for general convinicing arguments you wont need to state it.

Theorem. *Show there exists infinitley many primes p such that $p \equiv 3 \mod 4$*

12 Lecture 16 - Contradiction + induction

12.1 Contradiction

A prrof by contradiction of a statement P invloves the assumption of $\neg P$ and making an attempt to show that it is contradictory and so by LEM P must be true. Formally a contradiction is a statement of the form $(C \wedge \neg C)$

Theorem. *If* $0 < x < 1$ *then* $\frac{1}{x(1-x)} \geq 4$

Proof. Suppose for contradiction that we have $0 < x < 1$ and $\frac{1}{x(1-x)} < 4$

We may also note $0 < 1 - x < 1$. So we may then say $x(1-x) > 0$ So from the assumption we deduce that

$$\begin{aligned} 1 &< 4x(1-x) \\ 1 &< 4x - 4x^2 \\ 4x^2 - 4x + 1 &< 0 \\ (2x+1)^2 &< 0 \end{aligned}$$

But we know that for all $y \in \mathbb{R}$ that $y^2 \geq 0$ so we know that $(2x+1)^2 \geq 0$ yeilding a contradiction. □

12.2 Induction

Theorem. *Let* $P(n)$ *be a sequence of statements for all* $n \in \mathbb{N}$. *Suppose it is known that* $P(0)$ *holds and that* $P(k) \Rightarrow P(k+1)$ *holds then we may say* $\forall n \in \mathbb{N}, P(n)$

If instead we want to start the proof from another base case i.e. $P(n)$ for all $n \in \mathbb{N}, n \geq l$. Induction can still be used. Formally this would be proving a proposition $C(n) := P(n+l)$