Basic Logic

Math Swenton

We can build logical expressions from simpler ones via logical predicates and quantifiers, just as we combine numbers by arithmetic operations—but instead of numbers, our building blocks are logical ***propositions*** (statements of truth that are either *true* or *false*), and our operations are logical predicates such as "and", "or", "not", etc.

Predicates

Predicates play the role constants and functions in the realm of logic.

- Predicates take as input some number of propositions and, depending on their values, evaluate to either *true* or *false*.
  - As special cases, we have the *constant* predicates ***true*** and ***false*** themselves.
  - The basic higher-order predicates can be explicitly defined via truth tables:

not P:

P = T	P = F
F	T

P and Q:

	P = T	P = F
Q = T	T	F
Q = F	F	F

P or Q:

	P = T	P = F
Q = T	T	T
Q = F	T	F

$P \Rightarrow Q$:

	P = T	P = F
Q = T	T	T
Q = F	F	T

$P \Leftrightarrow Q$:

	P = T	P = F
Q = T	T	F
Q = F	F	T

- Note that "or" is *inclusive*—i.e., (*true* or *true*) is *true*. [We use "xor" for exclusive-or (very rarely).]
- The predicate "$\Rightarrow$" is read "implies"
  - "$P \Rightarrow Q$" means "If P, then Q"; we call P the ***hypothesis*** and Q the ***conclusion*** of the implication.
  - Note that this predicate is not symmetric—e.g., $P \Rightarrow Q$ is not equivalent to $Q \Rightarrow P$.
  - Also, note that *false* $\Rightarrow Q$ for *any* Q—i.e., a false hypothesis allows us to deduce anything we like!
- The predicate "$\Leftrightarrow$" is read "if and only if" (equivalent to "$\Leftarrow$ and $\Rightarrow$"); it serves as our "equal sign" for logical propositions.

Quantifiers

Quantifiers allow us to specify the roles of variables in a proposition:

- The ***universal quantifier*** $\forall$'s syntax is $\boxed{\forall x,\ P}$, read "for all x, P."
  This is *true* just when P is *true* for each and every value of x; it is *false* if even one choice of x makes P *false*.
- The ***existential quantifier*** $\exists$'s syntax is $\boxed{\exists x \text{ such that } P}$, read "there exists x such that P."
  This is *true* just when there is at least one value of x for which P is *true*; it is *false* if P is *false* for every choice of x.

The values allowed by a quantifier are often restricted implicitly (from context) or explicitly.

- e.g., "$\forall \varepsilon > 0,\ \exists \delta > 0 \ldots$" refers only to positive real numbers ε and δ.

Unquantified variables in an expression are called ***free variables***; by convention, free variables are universally quantified—be aware of free variables and make these quantifications explicit when necessary (particularly when negating a proposition).

Logical algebra

We can manipulate logical expressions just as we manipulate numerical ones, via the following rules:

Associativity	P and (Q and R) $\Leftrightarrow$ (P and Q) and R	P or (Q or R) $\Leftrightarrow$ (P or Q) or R
Commutativity	P and Q $\Leftrightarrow$ Q and P	P or Q $\Leftrightarrow$ Q or P
Distributivity	P and (Q or R) $\Leftrightarrow$ (P and Q) or (P and R)	P or (Q and R) $\Leftrightarrow$ (P or Q) and (P or R)
Units	P and *true* $\Leftrightarrow$ P $\Leftrightarrow$ P or *false*	
Negation	not *true* $\Leftrightarrow$ *false*	not(not P) $\Leftrightarrow$ P
	not(P and Q) $\Leftrightarrow$ (not P) or (not Q)	not(P or Q) $\Leftrightarrow$ (not P) and (not Q)
	not($\forall x,\ P$) $\Leftrightarrow$ $\exists x$ such that not P	not($\exists x$ such that P) $\Leftrightarrow$ $\forall x,$ not P
Implication	($P \Rightarrow Q$) $\Leftrightarrow$ (Q or not P)	$P \Rightarrow P$ or Q
	($P \Leftrightarrow Q$) $\Leftrightarrow$ ($P \Rightarrow Q$) and ($Q \Rightarrow P$)	P and $Q \Rightarrow P$
	not($P \Rightarrow Q$) $\Leftrightarrow$ P and not Q	

Other identities	*false* and P $\Leftrightarrow$ *false*	P and P $\Leftrightarrow$ P	P and (not P) $\Leftrightarrow$ *false*
	true or P $\Leftrightarrow$ *true*	P or P $\Leftrightarrow$ P	P or (not P) $\Leftrightarrow$ *true*

Modern mathematics centers on logical propositions (which may be either *true* or *false*) about mathematical concepts. Rather than judging such "truth" subjectively on the basis of faith or intuition, or relying on non-absolute methods such as experimental testing, in mathematics we demand that a proposition be justified by a *proof* in order to be accepted—once proven, a proposition achieves special status in mathematics and is often called a ***theorem*** (usually when it's a final result) or ***lemma*** (when it's a step toward something larger).

Aside: Mathematics is the study of logical relationships between mathematical concepts. Important concepts are given names and formal definitions in order to allow proper study of them, and proofs establish the logical connections between points of interest, providing us pathways of truth through the mathematical landscape. At first, we work with basic definitions and establish short logical pathways; building on this, we then establish theorems that allow us to jump greater logical distances in a single step; in turn, we use these theorems to prove larger theorems that span even greater logical distances, and so on... the result is a logical infrastructure in the mathematical landscape that which comprises our "understanding" of mathematics—including logical reasoning skills, concepts, definitions, theorems, and proofs.

Proof

A ***proof*** is a sequence of logical propositions, in which each proposition is logically justified by some combination of axioms, definitions, established theorems, and the propositions *preceding* it in the proof.

- The steps in a proof must build from start to finish.
- Proofs are not just about a proposition *being* true—they're about establishing the necessary connections to *justify* its truth.
  - If each step in a proof is valid, then the entire logical chain of the proof is valid.
  - Any improperly justified step in a proof invalidates the entire proof (even if the proposition itself is true!).
- A few tips to keep in mind when writing a proof:
  - Keep close track of what you already *know* (!) and what you're trying to *show* (?).
  - The first step of many proofs is to use *definitions* of terms to unravel them into the objects and logical propositions that they represent; once this has been done, these objects and propositions can be analyzed and combined to construct a proof.
  - Keep an eye out for any known *results* or *theorems* that relate to the proposition you're trying to prove—when something is already known about the concepts at play, a theorem can allow you to prove your proposition without unraveling definitions—this becomes increasingly important as the concepts being studied increase in complexity.

Proof techniques

Noting how the the structure of the proposition we'd like to prove is built from smaller propositions tells us a great deal about how to prove it:

- Each possible outermost logical construction leads us to a corresponding *direct* line of proof:
  - $\underline{\forall x,\ P}$: · "Let x be given." ← you must take the x that's given to you, not choose one yourself
    · Show that P is *true*.
  - $\underline{\exists x \text{ such that } P}$: [Find an x that makes P *true*] ← this is only scratch work, not part of the proof
    · "Let $x = \ldots$"
    · Show that P is *true* for this x.
  - $\underline{P \Rightarrow Q}$: · "Suppose P."
    · Show that Q is *true*.
  - $\underline{P \Leftrightarrow Q}$: Show $[P \Rightarrow Q \text{ and } Q \Rightarrow P]$ —or— connect P to Q via a chain of $\Leftrightarrow$'s.
- A proposition can also be proven *indirectly* by showing that its logical negation is *false*; the advantage that this sometimes provides is that negation changes the outermost operation of the expression, allowing a different line of attack.
- There are four common means of proving the most common type of mathematical assertion, the *implication* $\underline{P \Rightarrow Q}$:
  - Suppose P and show Q. (*directly*)
  - Suppose $[\text{not } Q]$ and show $[\text{not } P]$. (*by the contrapositive*)
  - Show that $[Q \text{ or not } P]$ is *true*. (*by definition*)
  - Suppose $[P \text{ and not } Q]$ and deduce a *false* proposition. (*by contradiction*)

Sets

A ***set*** is a collection of objects, such that any object x is either in the set (written $x \in S$) or not in the set (written $x \notin S$), but not both: $\boxed{S \text{ is a set } \Leftrightarrow \forall x,\ x \in S \text{ xor } x \notin S}$.

- Simple sets can be expressed simply by listing their elements — e.g., "the set $\{a,\ b,\ c\}$", or "the set $A = \{1,\ 2,\ 3,\ \ldots\}$".
- More complicated sets are often expressed via the notation $\{x : P(x)\}$, read "the set of all x such that $P(x)$."
  This allows us to collect all objects with some property into a set: $\boxed{a \in \{x : P(x)\} \text{ means "} P(a) \text{ is } \textit{true}\text{"}}$.
  - e.g., $a \in \left\{ x : x^2 - 3x + 2 = 0 \right\}$ simply means $a^2 - 3a + 2 = 0$.
- Some sets are expressed via the more intricate notation $\{f(x) : P(x)\}$, in which the left side isn't simply a variable.
  Here, the left side indicates the *form* of the set's elements, and the right side indicates the *credentials* required for inclusion into the set; in practical terms, $\boxed{a \in \{f(x) : P(x)\} \text{ means "} a = f(x) \text{, where } P(x) \text{ is } \textit{true}\text{"}}$.
  - e.g., $z \in \left\{ x + iy : x, y \in \mathbb{R} \text{ and } x^2 + y^2 = 1 \right\}$ means: $z = x + iy$, where $x, y \in \mathbb{R}$ and $x^2 + y^2 = 1$.
- Some common sets and the symbols used to represent them:
  - The ***empty set***: $\varnothing = \{\ \}$, i.e. the set containing no elements
  - Some important sets of numbers:
    - the ***natural numbers***, $\mathbb{N} = \{1,\ 2,\ 3,\ 4,\ \ldots\}$ and ***integers***, $\mathbb{Z} = \{\ldots,\ -2,\ -1,\ 0,\ 1,\ 2,\ \ldots\}$;
    - the ***rationals***, $\mathbb{Q} = \left\{ \dfrac{p}{q} : p, q \in \mathbb{Z} \text{ and } q \neq 0 \right\}$ and ***real numbers***, $\mathbb{R}$; and
    - the ***complex numbers***, $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ (where $i^2 = -1$).

Set Arithmetic

Numbers and logical propositions are not the only objects that can be manipulated and compared—similar operations exist for sets, which form the foundation of most objects that we study higher mathematics; the most important of these are listed below.

[In the formulæ below, uppercase letters represent sets and script letters represent collections of sets.]

Subsets	$A \subset B$ means $x \in A \Rightarrow x \in B$	
Equality	$A = B$ means $x \in A \Leftrightarrow x \in B$ [or, equivalently, $A \subset B$ and $B \subset A$]	
Union	$A \cup B \stackrel{\text{def}}{=} \{x : x \in A \text{ or } x \in B\}$	$\bigcup \mathcal{B} \stackrel{\text{def}}{=} \{x : \exists B \in \mathcal{B} \text{ such that } x \in B\}$
Intersection	$A \cap B \stackrel{\text{def}}{=} \{x : x \in A \text{ and } x \in B\}$	$\bigcap \mathcal{B} \stackrel{\text{def}}{=} \{x : \forall B \in \mathcal{B},\ x \in B\}$
Difference	$A \smallsetminus B \stackrel{\text{def}}{=} \{x : x \in A \text{ and } x \notin B\}$	
Cartesian product	$A \times B \stackrel{\text{def}}{=} \{(a, b) : a \in A \text{ and } b \in B\}$	
Power set	$\mathscr{P}(X) \stackrel{\text{def}}{=} \{A : A \subset X\}$ [so $s \in \mathscr{P}(X) \Leftrightarrow s \subset X$]	
Distributive laws	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cap \bigcup_{B \in \mathcal{B}} B = \bigcup_{B \in \mathcal{B}} (A \cap B)$
	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cup \bigcap_{B \in \mathcal{B}} B = \bigcap_{B \in \mathcal{B}} (A \cup B)$
DeMorgan's laws	$X \smallsetminus (A \cup B) = (X \smallsetminus A) \cap (X \smallsetminus B)$	$X \smallsetminus \bigcup_{B \in \mathcal{B}} B = \bigcap_{B \in \mathcal{B}} (X \smallsetminus B)$
	$X \smallsetminus (A \cap B) = (X \smallsetminus A) \cup (X \smallsetminus B)$	$X \smallsetminus \bigcap_{B \in \mathcal{B}} B = \bigcup_{B \in \mathcal{B}} (X \smallsetminus B)$
Emptiness	$A \neq \varnothing \Leftrightarrow \exists a \in A$	
	A and B are called ***disjoint*** if $A \cap B = \varnothing$	
	$\mathcal{C}$ is called a ***disjoint collection*** if $A, B \in \mathcal{C} \Rightarrow A = B$ or $A \cap B = \varnothing$	

Functions

- Suppose that X and Y are sets; formally, a ***function*** $f : X \to Y$ is a subset of $X \times Y$ having two properties:
  - $\forall\, x \in X,\ \exists\, y \in Y$ with $(x, y) \in f$ [every $x \in X$ has some corresponding $y \in Y$], and
  - $(x, y) \in f$ and $(x, y') \in f \;\Rightarrow\; y = y'$ [each $x \in X$ corresponds to just one $y \in Y$].

  For each $x \in X$, we denote this unique $y \in Y$ with $(x, y) \in f$ by $f(x)$.
- Independent of the formal definition above, the best way to think about a function $f : X \to Y$ is as an operation that picks up each element of X and ***maps*** it (sends it) to some element of Y:

  $$\boxed{\text{A function } f : X \to Y \text{ is a rule that assigns to each } x \in X \text{ exactly one value } f(x) \in Y}.$$
- The second property in the formal definition of function could be written as "$x = x' \;\Rightarrow\; f(x) = f(x')$"; in words, this says a function must be ***well-defined***, i.e., if you give it the same inputs, it produces the same outputs. We use this property all the time with little note—e.g., every time that we apply a function to both sides of an equation.
- We often express functions via expressions, as in "the function $f(x) = x^2 + 1$".
  - This should *not* be viewed as an equation, but rather, as a convenient way of expressing the *rule* $f : x \mapsto x^2 + 1$. In this case, the domain and codomain are often clear from context; however, it is always best to explicitly state the domain, codomain, and rule for a function, i.e.: "the function $f : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2 + 1$."
- Suppose that $f : X \to Y$ is a function; then we define the following terms:
  - The ***domain*** of f is X. [its set of input values]
  - The ***codomain*** of f is Y. [the set into which it sends its results—note that it need not fill that set!]
  - The ***range*** (or *image*) of f is the set $\{\, f(x) \;:\; x \in X \,\} \subset Y$ [the subset of Y that actually gets hit by f]
    - Note that this could be more clearly expressed as $\{\, y \in Y \;:\; \exists\, x \in X \text{ with } f(x) = y \,\}$.
  - f is ***injective*** means $f(x) = f(x') \;\Rightarrow\; x = x'$. [equivalently, that $x \neq x' \;\Rightarrow\; f(x) \neq f(x')$]
    - This means that no two distinct elements of x map to the same element of Y (a.k.a. f is "one-to-one").
  - f is ***surjective*** means that the range of f is all of Y. [equivalently, $\forall\, y \in Y,\ \exists\, x \in X$ with $f(x) = y$]
    - This means that every element of Y is "hit" by some element of X (a.k.a. f is "onto").
  - f is ***bijective*** means that f is both injective and surjective.
    - A bijective function $f : X \to Y$ *pairs* each element of X with exactly one element of Y, and vice-versa.

Image and Preimage

A function $f : X \to Y$ sends each element of X to some element of Y; equally important is the fact that a function can be used to map *sets* in *both directions*:

- If $A \subset X$, the ***image*** of A under f is defined as $\boxed{f[A] \stackrel{\text{def}}{=} \{\, f(a) \;:\; a \in A \,\}}$ (i.e., $\{\, y \in Y \;:\; \exists\, a \in A \text{ with } f(a) = y \,\}$).
  - That is, we let f throw each element of A, and $f[A]$ is the set of all of the elements of Y that result.
  - When taking the image of a subset $A \subset X$:
    - Each element of A must go somewhere, so *elements are not lost* during this process.
    - It's possible that some *collapsing* occurs due to the fact that two or more elements of A could map to the same element of Y (unless f is injective!).
  - Note that the range of a function $f : X \to Y$ is just $f[X]$, the image of *all* of X under f.
- If $B \subset Y$, the ***preimage*** of B under f is defined as $\boxed{f^{-1}[B] \stackrel{\text{def}}{=} \{\, x \in X \;:\; f(x) \in B \,\}}$.
  - That is, $f^{-1}[B]$ is the set of all elements of X that f maps into B.
  - When taking the preimage of a subset $B \subset Y$:
    - Any elements of B not in the range of f will be *lost* in the process (unless f is surjective!).
    - *Expansion* could occur, because some elements of B could come from multiple elements of X (unless f is injective!).

The image and preimage under a function f relate to one another in the following two ways:

- $\forall\, A \subset X,\ A \subset f^{-1}\big[f[A]\big]$ (with equality holding for all such A if and only if f is injective).
- $\forall\, B \subset Y,\ f\big[f^{-1}[B]\big] \subset B$ (with equality holding for all such B if and only if f is surjective).