A Logician's Toolbox

461: An Introduction to Mathematical Logic

Spring 2009

We recast/introduce notions which arise everywhere in mathematics.
All proofs are left as exercises.

0 Notations from set theory

- $\{1,2\} = \{2,1\} = \{1,2,1\}$
- The ordered pair (a,b) is the set $\{a,\{a,b\}\}$.
  One has $(a,b) = (c,d)$ iff $a = c$ and $b = d$.
- The Cartesian product of two sets A and B is
$$A \times B = \{(a,b) : a \in A, b \in B\}$$
- The power set of A is the set of all subsets of A,
$$P(A) = \{X : X \subseteq A\}$$
- When A and B are sets, B^A denotes the set of all functions $A \to B$.
- $0 \in \mathbb{N}$!

1 Functions

Definition 1.1 (function)**.** Function A function from A to B is a relation f on $A \times B$ such that:

$$\forall a \in A\ \forall b, b' \in B,\ (a,b) \in f \wedge (a,b') \in f \to b = b'$$

We then write $f : A \to B$, and $b = f(a)$ for $(a,b) \in f$.

When talking about a function, it is always very important to make clear its domain $\operatorname{dom} f$ and its codomain $\operatorname{cod} f$ (A and B respectively in the definition above). To indicate the mapping, the following notation is customary:

$$\begin{array}{rccc} f: & A & \to & B \\ & x & \mapsto & f(x) \end{array}$$

Definition 1.2 (composition)**.** Composition Let $f : A \to B$, $g : B \to C$ be functions. Their composition is the function $g \circ f : A \to C$ defined by:

$$(a, c) \in g \circ f \quad \text{if} \quad \exists b \in B \quad (a, b) \in f \wedge (b, c) \in g$$

In other words, $c = (g \circ f)(a)$ iff there is $b \in B$ such that $b = f(a)$ and $c = g(b)$ iff $c = g(f(a))$.

Properties 1.3. *Composition is associative. If $f : A \to B$, $g : B \to C$, $h : C \to D$ are functions, then $h \circ (g \circ f) = (h \circ g) \circ f$.*

1.1 Injections and Surjections

Definition 1.4 (injection)**.** Injection A function $f : A \to B$ is injective/an injection if

$$\forall a, a' \in A, \quad f(a) = f(a') \to a = a'$$

Notation 1.5. Injectivity of f is sometimes denoted $f : A \hookrightarrow B$.

Properties 1.6. *Let $f : A \to B$, $g : B \to C$ be functions.*

- *If f and g are injective, so is $g \circ f$.*
- *If $g \circ f$ is injective, so is f.*

Counter-example 1.7. Let f be the inclusion map from $\{0\}$ into $\{0, 1\}$, and g be the constant map from $\{0, 1\}$ to $\{0\}$. Then $g \circ f$ is the identity function of $\{0\}$, clearly injective, but g isn't.

Definition 1.8 (surjection)**.** Surjection A function $f : A \to B$ is surjective/a surjection if

$$\forall b \in B \quad \exists a \in A, \quad b = f(a)$$

Notation 1.9. Surjectivity of f is sometimes denoted $f : A \twoheadrightarrow B$.

Properties 1.10. *Let $f : A \to B$, $g : B \to C$ be functions.*

- *If f and g are surjective, so is $g \circ f$.*
- *If $g \circ f$ is surjective, so is g.*

Counter-example 1.11. In counter-example 1.7, $g \circ f$ is surjective, but f isn't.

1.2 Bijections

Definition 1.12 (bijection)**.** Bijection A function $f : A \to B$ is bijective/a bijection if it is both injective and surjective.

Properties 1.13. *Let $f : A \to B$, $g : B \to C$ be functions.*

- *If f and g are bijective, so is $g \circ f$.*
- *If $g \circ f$ is bijective, then f is injective and g is surjective.*

Proposition 1.14. *Let $f : A \to B$ be a bijection. Then there exists a unique function $g : B \to A$ such that $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_B$. Moreover, g is a bijection; it is called the reciprocal bijection of f and denoted f^{-1}.*

1.3 Image and Pre-image Sets

Definition 1.15 (Image set)**.** Image set Let $f : A \to B$ be a function and $X \subseteq A$ be a subset of A. The image of X under f is

$$f(X) = \{f(x) : x \in A\}$$

Properties 1.16. *Let $f : A \to B$ be a function and $X, Y \subseteq A$ subsets of A.*

- $f(X \cap Y) \subseteq f(X) \cap f(Y)$
- $f(X \cup Y) = f(X) \cup f(Y)$

Counter-example 1.17. Let $f : \{0, 1\} \to \{0\}$ be the constant function; set $X = \{0\}$ and $Y = \{1\}$. Then $X \cap Y = \emptyset$ but $f(X) \cap f(Y) = \{0\} \neq \emptyset$.

Exercise 1.18. Let $f : A \to B$ be a function and g defined as follows:

$$\begin{array}{rccc} g: & P(A) & \to & P(B) \\ & X & \mapsto & f(X) \end{array}$$

1. Show that f is injective iff g is.
2. Show that f is surjective iff g is.

Definition 1.19 (Pre-image set)**.** Pre-image Let $f : A \to B$ be a function and $X \subseteq B$ be a subset of B. The pre-image of X under f is

$$f^{-1}(X) = \{x \in A : f(x) \in X\}$$

Remark 1.20. f^{-1} as a function from B to A makes sense only when f is a bijection; f^{-1} as a function from $P(B)$ to $P(A)$ is always defined. It is the case that when f is bijective and $X \subseteq B$, one has

$$\underbrace{f^{-1}(X)}_{\text{Image under } f^{-1}} \quad = \quad \underbrace{f^{-1}(X)}_{\text{Pre-image under } f}$$

Properties 1.21. *Let $f : A \to B$ be a function and $X, Y \subseteq B$ subsets of B.*

- $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$
- $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$

The following is dual to Exercise 1.18.

Exercise 1.22. Let $f : A \to B$ be a function and h defined as follows:

$$\begin{array}{rccc} h: & P(B) & \to & P(A) \\ & X & \mapsto & f^{-1}(X) \end{array}$$

1. Show that f is injective iff h is surjective.
2. Show that f is surjective iff h is injective.

1.4 Their interplay

Exercise 1.23. Let $f : A \to B$ be a function.

1. Let $X \subseteq A$. Show that $f^{-1}(f(X)) \subseteq X$.
2. Suppose that f is injective. Show $\forall X \subseteq A, f^{-1}(f(X)) = X$
3. Suppose $\forall X \subseteq A, f^{-1}(f(X)) = X$ Show that f is injective.

Exercise 1.24. Let $f : A \to B$ be a function.

1. Let $X \subseteq B$. Show that $X \subseteq f(f^{-1}(X)$.
2. Suppose that f is surjective. Show $\forall X \subseteq B, f(f^{-1}(X)) = X$.
3. Suppose $\forall X \subseteq B, f(f^{-1}(X)) = X$. Show that f is surjective.

2 Equivalence Relations

2.1 Equivalence Relations

Definition 2.1 (equivalence relation)**.** Equivalence relation An equivalence relation on a set A is a relation $\sim\subseteq A \times A$ which is reflexive, symmetric, and transitive. We write of course $a \sim b$ instead of $(a, b) \in\sim$. Hence the definition is:

- $\forall a \in A,\ a \sim a$ (reflexivity)
- $\forall a, b \in A,\ a \sim b \to b \sim a$ (symmetry)
- $\forall a, b, c \in A,\ a \sim b \wedge b \sim c \to a \sim c$ (transitivity)

Definition 2.2 (equivalence class)**.** Let $\sim$ be an equivalence relation on a set A. Let $a \in A$. Then the equivalence class of a modulo $\sim$ is the set

$$[a]_\sim = \{b \in A : a \sim b\}$$

One may drop the subscript $\sim$ if there is no risk of ambiguity.

Properties 2.3. *Let $\sim$ be an equivalence relation on a set A. Let $a, b \in A$. Then $a \sim b$ iff $a \in [b]_\sim$ iff $b \in [a]_\sim$ iff $[a]_\sim \cap [b]_\sim \neq \emptyset$.*

Definition 2.4 (quotient set)**.** Quotient set Let $\sim$ be an equivalence relation on a set A. The quotient set of A by $\sim$ is the set of all equivalence classes:

$$A/\sim = \{[a]_\sim : a \in A\}$$

2.2 Partitions

Definition 2.5 (partition)**.** Partition Let A be a set. A partition of A is a subset Π of $P(A)$ such that:

- $\emptyset \notin \Pi$ (no member of Π is empty)
- $\bigcup \Pi = A$ (members of Π cover A)
- $\forall X, Y \in \Pi,\ X \cap Y \neq \emptyset \to X = Y$ (distinct members of Π don't overlap).

The typical example is that of the set of classes of an equivalence relation.

Remark 2.6. Let $\sim$ be an equivalence relation on A. Then $A/\sim$ is a partition of A.

This is no coincidence.

Proposition 2.7. *Let A be a set. Then there is a bijection between the set of equivalence relations on A and the set of partitions of A.*

3 Order Relations

3.1 Pre-orderings

Definition 3.1 (pre-ordering)**.** Pre-ordering A pre-ordering on a set A is a relation $\precsim$ which is reflexive and transitive.

- $\forall a \in A,\ a \precsim a$ (reflexivity)
- $\forall a, b, c \in A,\ a \precsim b \wedge b \precsim c \to a \precsim c$ (transitivity)

These tend to occur in a mathematician's everyday life, though they are fairly loose relations.

Notice that no one said that elements a and b could always be compared: perhaps neither $a \precsim b$ nor $b \precsim a$ holds. The dullest example of a pre-ordering is the empty relation, that is no two elements are in relation.

When $a \precsim b \wedge b \precsim a$, one says that a and b can be compared.

3.2 Partial Orderings

Definition 3.2 (ordering, poset)**.** OrderingPoset An ordering on a set A is a pre-ordering $\preceq$ which is anti-symmetric.

- $\forall a \in A,\ a \precsim a$ (reflexivity)
- $\forall a, b \in A,\ a \preceq b \wedge b \preceq a \to a = b$ (anti-symmetry)
- $\forall a, b, c \in A,\ a \precsim b \wedge b \precsim c \to a \precsim c$ (transitivity)

One then says that $(A, \preceq)$ is a poset.

Of course there is a way to retrieve an ordering from any pre-ordering; it suffices to say that elements which both lie above each other must actually be equal. This is done by "factoring out" the natural equivalence relation.

Proposition 3.3. *Let $\precsim$ be a pre-ordering on a set A. Then*

- *The relation $\sim$ defined by*

$$a \sim b \quad \textit{if} \quad a \precsim b \wedge b \precsim a$$

  is an equivalence relation on A.

- *The relation $\preceq$ defined by*

$$[a]_\sim \preceq [b]_\sim \quad \textit{if} \quad a \precsim b$$

  is an ordering relation on $A/\sim$.

- *The relation $\preceq$ defined above is the only order relation on $A/\sim$ which is compatible with $\precsim$.*

Notice that there is still no reason for any two elements to be comparable.

3.3 Minimal and Least Elements

Definition 3.4 (minimal element)**.** Minimal Element Let $(A, \preceq)$ be a poset. $a \in A$ is a minimal element if $\forall b \in A\ b \preceq a \to b = a$.

Minimal elements need not exist; when they do, they need not be unique.

Counter-example 3.5. Consider $A = \{1, 2\}$ with the trivial ordering (x can be compared only with x). Both 1 and 2 are minimal.

One defines maximal similarly.

Definition 3.6 (least element)**.** Least Element Let $(A, \preceq)$ be a poset. $a \in A$ is the least element of A if $\forall b \in A\ b \neq a \to a \prec b$.

This need not exist, but if it does, it is unique.

Remark 3.7. If there is a least element, it is unique.

One defines greatest element similarly.

Definition 3.8 (upper bound, bounded above)**.** Upper BoundBounded Above Let $(A, \preceq)$ be a poset and $X \subseteq A$. $a \in A$ is an upper bound for X if $\forall x \in X\ x \preceq a$. X is said to be bounded above (by a).

a need of course not be unique (any $b \succ a$ does too).

Remark 3.9. A is bounded above in A iff A has a greatest element.

One defines lower bound similarly.

Definition 3.10 (least upper bound)**.** Let $(A, \preceq)$ be a poset and $X \subseteq A$. $a \in A$ is a least upper bound for X if it is an upper bound for X, and $\forall b \in A$, b is an upper bound for $X \to b \succeq a$.

One also says that a is the supremum of X.

Remark 3.11. If X has a least upper bound, it is unique.

Not all sets bounded above have a least upper bound.

Counter-example 3.12. Consider the poset $(\mathbb{Q}, \leq)$. Then $\{q \in \mathbb{Q} : q^2 < 2\}$ is bounded above, but has no least upper bound.

One defines greatest lower bound similarly.

Exercise 3.13. Write formal definitions for: maximal element, greatest element, lower bound, greatest lower bound.

3.4 Linear Orderings and Extensions

Definition 3.14 (linear ordering)**.** Linear Ordering A linear/total ordering on A is an ordering $\leq$ such that any two elements are comparable.

- $\forall a, b \in A,\ a \leq b \wedge b \leq a$ (linearity)

Definition 3.15 (extension)**.** Let R, S be relations on a set A. S extends R is $R \subseteq S$.

Remark 3.16. Let A be a finite set and R an ordering on A. Then there is a linear ordering S on A extending R.

The general case is a consequence of compactness theorems in logic.

4 Cardinalities

4.1 Equinumerosity

Definition 4.1 (equinumerosity)**.** Equinumerous Two sets A, B are equinumerous if there is a bijection $f : A \to B$. This is written $A \approx B$.

Properties 4.2. *Equinumerosity is reflexive, symmetric, and transitive.*

- $\forall A,\ A \approx A$
- $\forall A, B,\ A \approx B \to B \approx A$
- $\forall A, B, C,\ A \approx B \wedge B \approx C \to A \approx C$

Equinumerosity thus behaves very much like an equivalence relation (Definition 2.1), except of course that the collection of all sets is not a set itself.

Definition 4.3 (domination)**.** Domination A set A is dominated by a set B if there is an injection $f : A \to B$. We then write $A \precsim B$.

Properties 4.4. *Domination is reflexive and transitive.*

- $\forall A,\ A \precsim A$
- $\forall A, B, C,\ A \precsim B \wedge B \precsim C \to A \precsim C$

Domination behaves very much like a pre-ordering (Definition 3.1) - with the same proviso that the collection of all sets is not a set.

Two facts are remarkable. First, the equivalence relation associated to the pre-ordering is equinumerosity (Theorem 4.5). Second, it is (modulo the relation) a linear ordering, meaning that two sets are always comparable (Theorem 4.6). The second is actually equivalent to the axiom of choixe, but the first holds true even without AC.

Theorem 4.5 (Cantor-Bernstein)**.** *Cantor-Bernstein Theorem Let A, B be sets such that $A \precsim B$ and $B \precsim A$. Then $A \approx B$. In other words, if there exist an injection $A \hookrightarrow B$ and an injection $B \hookrightarrow A$, then there is a bijection $A \approx B$.*

Theorem 4.6 (Comparability; uses AC)**.** *Comparability Theorem Let A, B be sets. Then $A \precsim B$ or $B \precsim A$. In other words, there exists an injection $A \hookrightarrow B$ or an injection $B \hookrightarrow A$.*

4.2 Cardinals

Fact 4.7 (Uses AC)**.** *There is a notion of cardinal, that is for any set A there is a set* $\operatorname{Card} A$ *such that:*

- $A \precsim B$ *iff* $\operatorname{Card} A \leq \operatorname{Card} B$
- $A \approx B$ *iff* $\operatorname{Card} A = \operatorname{Card} B$
- $\operatorname{Card}(\operatorname{Card} A) = \operatorname{Card} A$

Notation 4.8. $\operatorname{Card} \mathbb{N}$ is denoted $\aleph_0$. $\operatorname{Card} 2^{\mathbb{N}}$ is denoted $2^{\aleph_0}$.

Definition 4.9 (countable)**.** Countable A set is countable if its cardinal is $\aleph_0$.

4.3 Some computations

Proposition 4.10. *For every set A, $P(A) \approx 2^A$.*

In particular $\operatorname{Card} P(\mathbb{N}) = 2^{\aleph_0}$.

Theorem 4.11 (Cantor)**.** *For every set A, $P(A) \succ A$ (meaning $A \precsim P(A)$ but $A \not\approx P(A)$).*

Proposition 4.12. *$\mathbb{Z}$, $\mathbb{N}^2$, $\mathbb{Q}$ are countable.*

Proposition 4.13.

- *A countable union of countable sets is countable.*
- *The set of finite sequences of a countable set is countable.*
- *The set of eventually constant sequences of a countable set is countable.*

A sequence $(a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$ is eventually constant if

$$\exists a \in A \; \exists n_0 \in \mathbb{N} \; \forall n \in \mathbb{N} \quad n \geq n_0 \to a_n = a$$

Exercise 4.14.

- The set of decreasing functions $\mathbb{N} \to \mathbb{N}$ is countable.
- The set of strictly increasing functions $\mathbb{N} \to \mathbb{N}$ is equinumerous to $P(\mathbb{N})$.

Proposition 4.15. $(0,1) \approx \mathbb{R} \approx P(\mathbb{N})$.

In particular, $\operatorname{Card}\mathbb{R} = 2^{\aleph_0}$.

Cantor's Theorem (Theorem 4.11) says that $2^{\aleph_0} > \aleph_0$. It is then fairly natural to ask whether there is some cardinal number in between. In view of our results, this amounts to asking if all subsets of $\mathbb{R}$ not equinumerous to $\mathbb{R}$ are countable or not.

Continuum Hypothesis (CH). *Every subset of* $\mathbb{R}$ *not equinumerous to* $\mathbb{R}$ *is countable.*

This statement is equiconsistent to ZF+AC, meaning that it can neither be proved nor refuted.