Mathematical Objects

Mathematical assertions can be regarded as statements about objects in some abstract "mathematical universe"; *e.g.*:

Sets: Represent (unordered) collections of objects (perhaps other sets).

Functions: Abstract the idea of a "black box" that takes an object as input and produces an object as output.

Relations: Abstract the idea of a property that can be true or false of an object or sequence of objects.

Ordered pairs and tuples: Represent sequences (ordered collections) of objects.

Natural numbers: $0, 1, 2, 3, \ldots$. Usually considered together with operations such as $+$ $*$.

Sets

Sets can be considered "the data structures of mathematics".

- All normal mathematical objects can be constructed from "*pure sets*."
- The logic of sets can be formalized as a relatively small set of axioms and inference rules.
- The standard version of set theory is called *ZFC* (Zermelo-Fraenkel set theory with Choice).
- Most working mathematicians assume ZFC as their foundation.
- Mostly, we can work "naively" with sets, without having to worry about axiomatics.

Properties of Sets

Set theory can be formulated as a "first-order" logic with predicates $=$ (equality) and $\in$ (element of). Basic properties are:

Extensionality: Two sets are equal if and only if they have the same elements:

$$\forall A\ B.\ A = B \leftrightarrow (\forall X.\ X \in A \leftrightarrow X \in B).$$

Def: $A \subseteq B \ \equiv\ \forall X.\ X \in A \to X \in B$.

Comprehension: Given a set A and a predicate P, there is a set B whose elements are precisely those elements of A that satisfy P:

$$\forall A.\ \exists B.\ (\forall X.\ X \in B \leftrightarrow X \in A \wedge P(X)).$$

Def: $\{X \in A.\ P(X)\} \ \equiv$ *the set asserted to exist*.

Note that it will be unique, due to extensionality.

Empty set: There exists a set with no elements:

$$\exists A.\ \forall X.\ X \notin A.$$

Def: ϕ *or* $\{\} \ \equiv$ *the set asserted to exist.*

Pairing: Given sets A and B, there exists a set having A and B as its only members:

$$\forall A\ B.\ \exists C.\ \forall X.\ X \in C \leftrightarrow (X = A \vee X = B).$$

Given $A\ B$, the set C is the *unordered pair* $\{A, B\}$.

Union: Given sets A and B, there exists a set having as members exactly those sets that are either a member of A or a member of B:

$$\forall A\ B.\ \exists C.\ \forall X.\ X \in C \leftrightarrow (X \in A \vee X \in B).$$

Def: $A \cup B \quad \equiv \quad$ *the set asserted to exist.*

Intersection: Given sets A and B, there exists a set having as members exactly those sets that are a member of both A and B:

$$\forall A\ B.\ \exists C.\ \forall X.\ X \in C \leftrightarrow (X \in A \wedge X \in B).$$

Def: $A \cap B \quad \equiv \quad$ *the set asserted to exist.*

“Big-$\bigcup$”: Given A, there is a set having as its elements precisely those sets that are elements of *some* element of A:

$$\forall A.\ \exists B.\ \forall X.\ X \in B \leftrightarrow (\exists Y.\ Y \in A \wedge X \in Y).$$

Def: $\bigcup A \quad \equiv \quad$ *the set asserted to exist.*

“Big-$\bigcap$”: Given A, there is a set having as its elements precisely those sets that are elements of *all* elements of A:

$$\forall A.\ \exists B.\ \forall X.\ X \in B \leftrightarrow (\forall Y.\ Y \in A \rightarrow X \in Y).$$

Def: $\bigcap A \quad \equiv \quad$ *the set asserted to exist.*

Powerset: Given A, there is a set having as its elements precisely those sets that are subsets of A:

$$\forall A.\ \exists B.\ \forall X.\ X \in B \leftrightarrow X \subseteq A.$$

Def: $\mathcal{P}(A) \equiv$ *the set asserted to exist.*

From the empty set and powerset axioms, we can prove the existence of *lots* of sets:

$$\begin{aligned}
\mathcal{P}(\phi) &= \{\phi\} \\
\mathcal{P}(\mathcal{P}(\phi)) &= \{\phi, \{\phi\}\} \\
\mathcal{P}(\mathcal{P}(\mathcal{P}(\phi))) &= \{\phi, \{\phi\}, \{\{\phi\}\}, \{\phi, \{\phi\}\}\} \\
\ldots &
\end{aligned}$$

Derived Constructions

Various "encoding tricks" can be used to define standard mathematical constructions in terms of sets; *e.g.*:

Ordered Pair: Given A, there is a set having $\{A\}$ and $\{A, B\}$ as its only members:

$$\forall A\ B.\ \exists C.\ \forall X.\ X \in C \leftrightarrow X = \{A\} \vee X = \{A, B\}.$$

Def: $(A, B) \ \equiv$ *the set asserted to exist.*

Sets A and B are uniquely determined by (A, B)
(*i.e.* the property we want an ordered pair to satisfy holds).

Cartesian Product: Given A and B, there is a set having as its members precisely the ordered pairs (X, Y) where $X \in A$ and $Y \in B$:

$$\forall A\ B.\ \exists C.\ \forall Z.\ Z \in C \leftrightarrow$$
$$(\exists X\ Y.\ X \in A \wedge Y \in B \wedge Z = (X, Y)).$$

Def: $A \times B \quad \equiv \quad$ *the set asserted to exist.*

We can iterate this construction to define:

$$A_1 \times (A_2 \times A_3)$$
$$A_1 \times (A_2 \times (A_3 \times A_4)))$$
$$A_1 \times (A_2 \times (A_3 \times (A_4 \times A_5))))$$
$$\ldots$$

The elements of these sets are *lists*: (X_1, X_2, X_3), (X_1, X_2, X_3, X_4), $(X_1, X_2, X_3, X_4, X_5)$, *etc.*

The Natural Numbers

Another encoding trick can be used to define the natural numbers as sets:

$$\begin{array}{lll} 0 & = \phi & = \{\} \\ 1 & = \{\phi\} & = \{0\} \\ 2 & = \{\phi, \{\phi\}\} & = \{0, 1\} \\ 3 & = \{\phi, \{\phi\}, \{\phi, \{\phi\}\}\} & = \{0, 1, 2\} \\ \ldots & & \end{array}$$

The *successor* of a number is defined to be the set whose elements are that number and all of its elements:

Def: $S(X) \equiv X \cup \{X\}$

Infinity: There exists a set X such that ϕ in X and such that whenever Y in X, then also $S(Y) \in X$:

$$\exists X.\ \phi \in X \wedge (\forall Y.\ Y \in X \rightarrow S(Y) \in X).$$

Def: $\mathcal{N} \quad \equiv \quad$ *the smallest such set (w.r.t. $\subseteq$).*

Don't assign too much importance to these particular encoding tricks – other versions are possible.

The point is that the properties of sets are given by a few axioms, which means we don't need additional axioms for other concepts (such as ordered pairs, numbers, lists, *etc.*) if we can *define* them in terms of sets.

Set Theory: Some History

Set theory was invented by Georg Cantor and Richard Dedekind in the late 1800's:

- The theory was originally used in a "naive" (non-axiomatic) form.
- Cantor was able to formulate many mathematical notions in terms of sets.

- The need for a formal axiomatic theory became evident with the discovery of paradoxes in "Cantor's Paradise"; *e.g.*
  - **Russell's Paradox:** "Let A be the *set of all sets*. Let $P(X)$ be the property of sets which holds of a set X exactly when *X is not an element of X*. Form the set $B = \{X \in A.\ P(X)\}$. Then B contains all sets that are not members of themselves. *Is B a member of itself?*"
- The resolution of the paradoxes involved specifying careful restrictions on what could be considered to be a set. These rule out the existence of: "the set of all sets."

The point here is: set theory is far from trivial, even though "high school presentations" make it seem to be.

Functions

The intuitive idea of a function is that of a “black box”, which takes an input from some *domain* and produces an output in some *codomain*.

For each input, there is one and only one possible output.

- The concept of function is much older than that of a set.
- In set theory, functions are defined in terms of sets, rather than taken as primitive.
- Mathematics can also be based upon a theory of “pure functions”, as opposed to sets (*e.g.* Church’s λ-calculus).

Relations and Functions as Sets

Given sets A and B, a *binary relation* on A and B is defined to be a subset R of the cartesian product $A \times B$; *e.g.*

$$\begin{aligned} A &= \{1,2,3\} \\ B &= \{4,5\} \\ A \times B &= \{(1,4),(1,5),(2,4),(2,5),(3,4),(3,5)\} \\ R &= \{(1,5),(3,5),(2,4)\} \subseteq A \times B \end{aligned}$$

A *function* from A to B is a binary relation $F \subseteq A \times B$ such that:

$$\forall a.\ a \in A \to \exists! b.\ b \in B \wedge (a,b) \in F.$$

Here $\exists!$ means "there exists unique" and $\exists! x.\ P(x)$ abbreviates:

$$(\exists x.\ P(x)) \wedge (\forall x\ y.\ P(x) \wedge P(y) \to x = y).$$

Special Classes of Functions

A function F from A to B is:

- *One-to-one*, or *injective*, if

$$\forall a\ a'\ b.\ (a,b) \in F \land (a',b) \in F \rightarrow a = a'.$$

- *Onto*, or *surjective*, if

$$\forall b.\ b \in B \rightarrow (\exists a.\ (a,b) \in F).$$

- A *one-to-one correspondence*, or *bijective*, if it is both injective and surjective; or equivalently:

$$\forall b.\ b \in B \rightarrow (\exists! a.\ (a,b) \in F).$$

Using Functions to Compare Sets

- Sets A and B are *equinumerous* $|A| = |B|$ if there exists a bijection from A to B.
- Set A has *smaller cardinality* than B $(|A| \le |B|)$ if there exists an injection from A to B.
  - *Cantor-Schröder-Bernstein Theorem:* $|A| \le |B|$ and $|B| \le |A|$ implies $|A| = |B|$. (Not as trivial as it looks!)
  - *Pigeonhole Principle:* If $|A| < |B|$ (*i.e.* $|A| \le |B|$ but not $|A| = |B|$), then there is no injection from B to A. ("If $m < n$ and you put n pigeons in m holes, then some hole contains more than one pigeon.")

Finite and Infinite Sets

Characteristic properties of finite versus infinite sets:

- *No* finite set can be placed into one-to-one correspondence with a proper subset of itself.
- *Every* infinite set can be placed into one-to-one correspondence with some proper subset of itself.
  (*e.g.* $n \mapsto 2n$ on natural numbers)

Actually, in set theory these are used as the *definitions* of finite and infinite:

Def: A set A is *finite* if every injection $f : A \to A$ is also a surjection. A set that is not finite is called *infinite*.

Theorem: A set is finite if and only if it is equinumerous with some proper initial segment of the natural numbers.

e.g.

$$\{\texttt{red}, \texttt{blue}, \texttt{green}\} \leftrightarrow \{0, 1, 2\}$$

Countable and Uncountable Sets

Def: A set is *countably infinite* if it is equinumerous with the set $\mathcal{N}$ of *all* natural numbers. A set is *countable* if it is finite or countably infinite. A set is *uncountable* if it is not countable.

The bijection $n \mapsto 2n$, called an *enumeration* of the set of even numbers, shows that the set of even numbers is countably infinite.

Theorem: A set A is countable if and only if there is a *surjection* $f : \mathcal{N} \to A$.

The surjection f is called an *enumeration with repetition*.

Countability of the Rational Numbers

Theorem: The set of rational numbers is countable.

Proof: Every rational number can be represented as a fraction p/q (not unique), where p and q are natural numbers, and q is not 0. We can construct an enumeration with repetition of all the fractions:

$$0/1,\ 1/1,\ 0/2,\ 2/1,\ 1/2,\ 0/3,\ 3/1,\ 2/2,\ 1/3,\ 0/4,\ \ldots$$

p/q	1	2	3	...
0	0/1	0/2	0/3	...
1	1/1	1/2	1/3	...
2	2/1	2/2	2/3	...
3	3/1	3/2	3/3	...
...				

Existence of Uncountable Sets

Theorem: The set B of all functions $f : \mathcal{N} \to \{0, 1\}$ is uncountable.

Proof (using Cantor's diagonal argument):
Assume (justification?) that B is countable.
Choose (justification?) enumeration $f_0, f_1, f_2, \ldots$ of the elements of B.

Consider the following table:

$f_i(j)$	0	1	2	3	...
f_0	$f_0(0)$	$f_0(1)$	$f_0(2)$	$f_0(3)$	...
f_1	$f_1(0)$	$f_1(1)$	$f_1(2)$	$f_1(3)$	...
f_2	$f_2(0)$	$f_2(1)$	$f_2(2)$	$f_2(2)$	...
f_3	$f_3(0)$	$f_3(1)$	$f_3(2)$	$f_3(3)$	...
...					

Define $f : \mathcal{N} \to \{0, 1\}$ so that $f(k) = 1 - f_k(k)$. Then *f cannot be one of the f_i*, so not all functions $f : N \to \{0, 1\}$ are included among the f_i; contradicting our assumption. We conclude B is uncountable.

A more general version of this argument shows:

Theorem: For all sets A, we have $|A| < |\mathcal{P}(A)|$.

i.e. no set A is equinumerous with its own powerset $\mathcal{P}(A)$.

More about Binary Relations

A binary relation $R \subseteq A \times A$ is called:

- *reflexive* if $\forall a.\ a \in A \rightarrow (a, a) \in R$.
- *symmetric* if $\forall a\ b.\ (a, b) \in R \rightarrow (b, a) \in R$.
- *antisymmetric* if $\forall a\ b.\ (a, b) \wedge (b, a) \in R \rightarrow a = b$.
- *transitive* if $\forall a\ b\ c.\ (a, b) \in R \wedge (b, c) \in R \rightarrow (a, c) \in R$.
- an *equivalence* if it is reflexive, symmetric, and transitive.
- a *partial order* if it is reflexive, transitive, and antisymmetric.
- a *total (or linear) order* if it is a partial order, and in addition satisfies *dichotomy*: $\forall a\ b.\ (a, b) \in R \vee (b, a) \in R$.

Examples:

Example: $R = \{(m,n) \in \mathcal{N} \times \mathcal{N}.$ m = n *(mod 3)*$\}$ is an equivalence relation.

Example: $R = \{(m,n) \in \mathcal{N} \times \mathcal{N}.\ m \leq n\}$ is a total order.

Example: $R = \{(m,n) \in \mathcal{N} \times \mathcal{N}.\ m$ `evenly divides` $n\}$ is a partial order.

Alphabets and Strings

Def: An *alphabet* is a *nonempty* finite set.
(we call the elements "symbols")

Def: Let Σ be an alphabet. A *string "over"* Σ is a finite sequence $w = w_1 w_2 \ldots w_n$, where each $w_i \in \Sigma$.

- The number n is called the *length* $|w|$ of string w.
- The *empty string* $(n = 0)$ is denoted by ϵ.
- The set of all strings over Σ is denoted by Σ^*.

If we wanted to, we could *define* $\Sigma^* = \bigcup\{\Sigma^n : n \in \mathcal{N}\}$, but such details are not so important for us.

String Notation

- The ith symbol in string w $(1 \leq i \leq |w|)$ is $w(i)$.
- The *concatenation* of strings u and v is the string uv such that:
  1. $|uv| = |u| + |v|$
  2. $uv(i) = u(i)$, for $1 \leq i \leq |u|$
  3. $uv(i) = v(i - |u|)$, for $|u| + 1 \leq i \leq |u| + |v|$.
- Concatenation of strings is *associative*: and it has the empty string as an *identity*:

$$\forall u \ v \ w.\ (uv)w = u(vw) \qquad \forall u.\ u\epsilon = u = \epsilon u.$$

(Algebraically, $(\Sigma^*, \cdot, \epsilon)$ is a *monoid*)

Cardinality of Σ^*

Theorem: If Σ is an alphabet, then Σ^* is countably infinite.

Proof: We can enumerate Σ^* in *lexicographic order*:

- Choose an enumeration $\{x_1, x_2, \ldots, x_n\}$ of Σ. (justification?)
- Extend to an enumeration of Σ^*, by the following rules:
  - For each k, all strings of length k are enumerated before strings of length $k+1$.
  - The n^k strings of length exactly k are enumerated so that $v_1 \ldots v_k$ precedes $w_1 \ldots w_k$ provided that for some i with $0 \leq i < k$, we have $v_j = w_j$ for all $j < i$ and $v_{i+1} < w_{i+1}$ (order based on "first mismatch").

Languages

Def: If Σ is an alphabet, then a subset of Σ^* is called a *language "over" Σ*. Important examples of languages:

- ϕ – the *empty language*.
- Σ^* – the language containing every string.
- $\{w\}$ – the *singleton language* containing w.
- Σ – the language consisting of all single-symbol strings. (We are "punning" here, regarding $\Sigma \subseteq \Sigma^*$.)

As they are sets, we can form unions, intersections, and complements (with respect to Σ^*) of languages.

The Set of All Languages (over Σ)

The set of all languages over alphabet Σ is just $\mathcal{P}(\Sigma^*)$, the powerset of Σ^*.

Theorem: If Σ is an alphabet, then $\mathcal{P}(\Sigma^*)$ is uncountable.

Proof: We have already noted (by Cantor's Diagonal Argument) that $|A| < |P(\mathcal{A})|$ for *any* set A.