ZERMELO–FRAENKEL SET THEORY

James T. Smith
San Francisco State University

The units on set theory and logic have used ZF set theory without specifying precisely what it is. To investigate which arguments are possible in ZF and which not, you must have a precise description of it.

A major question asked during the development of ZF was what system of logic should be used as its framework. Logicians eventually agreed that the framework itself should not depend very much on set-theoretic reasoning. Investigators could then focus on the difficult problems of set theory: there would be little interplay between the framework and the subject under study. During 1920–1940, first-order logic crystallized as a convenient framework for the study of algebraic structures. *Applying* it does not require use of techniques commonly regarded as set-theoretic. Moreover, the Gödel completeness theorem shows that it encompasses (but doesn't necessarily simulate) many arguments that mathematicians commonly use to prove theorems expressed in a first-order language. Thus, to facilitate investigation of the scope of set theory, it seems appropriate to express it in a first-order language, and restrict it to use logic that is compatible with the first-order framework. When we *apply* set theory formulated that way, we can highlight the use of its major principles. They're explicitly stated in first-order set-theoretic axioms, and explicitly mentioned in first-order proofs. To be sure, some very elementary parts of set theory are involved in the underlying logical framework, necessary even to formulate those axioms and proofs. But the more powerful set-theoretic principles are displayed conspicuously.

ZF is formulated in a first-order theory with minimal apparatus:

- countably many variables, which we regard as varying over all sets;
- no constants;
- no operators;
- just two predicates, equality and the binary *membership* predicate $\in$.

The nonlogical axioms of ZF can be reduced to a small number, as follows.

extensionality	power set	choice
separation	pair set	foundation
replacement	union	infinity

The ZF axioms are kept to the minimum number in order to simplify studies of their properties. The list can be pared even further by deriving some axioms from others, but those arguments are uninformative. Each of these axioms is stated below in detail, with some remarks to show how the axioms are used to develop formally the set theory used in the various other units.

Extensionality: $\forall x \forall y (\forall w (w \in x \Leftrightarrow w \in y) \Rightarrow x = y)$

This was stated explicitly in the *Basic Set Theory* unit. The corresponding statement with $\Leftarrow$ in place of $\Rightarrow$ is a consequence of logical axioms.

Separation: The separation principle is a family of formulas that contains, for any variables y, s, x and each formula P with no free occurrence of s,

$$\forall y \exists s \forall x (x \in s \Leftrightarrow (x \in y \ \& \ P))$$

To interpret that, regard P as describing a property that may hold for some objects x. The principle says that given a set y there is a set s containing just those members of y for which P holds. This principle was stated explicitly in the *Basic Set Theory* unit. By the extensionality axiom, the set s is unique; it's usually denoted by $\{x \in y : P\}$.

The separation principle can in fact be deduced from the other axioms. That argument, which relies mostly on the replacement principle, is uninformative.

$\exists y (y = y)$ is a consequence of the axioms of elementary logic. Use that to obtain y, then apply the separation axiom with formula P: $x \neq x$. That yields a set s such that $\forall x (x \notin s)$. By the extensionality axiom, s is unique; it's usually denoted by ϕ.

Given sets y, z apply the separation axiom with formula P: $x \in z$. That yields a set s such that $\forall x (x \in s \Leftrightarrow (x \in y \ \& \ x \in z))$. By the extensionality axiom, s is unique; it's usually denoted by $y \cap z$.

Given a set $S \neq \phi$, deduce $\exists y (y \in S)$ to obtain y. Apply separation with formula P: $\forall z (z \in S \Rightarrow x \in z)$. That yields a set s such that $\forall x (x \in s \Leftrightarrow \forall z (z \in S \Rightarrow x \in z))$. By the extensionality axiom, s is unique; it's usually denoted by $\bigcap S$.

Replacement: This family of axioms contains, for any variables d, x, y, y', r and each formula F with no free occurrence of r,

$$\forall d (\forall x \forall y \forall y' (x \in d \ \& \ F \ \& \ F^{y}_{y'} \Rightarrow y = y') \Rightarrow \exists r \forall y (y \in r \Leftrightarrow \exists x (x \in d \ \& \ F)))$$

To interpret that, regard F as describing a relation that may hold between arguments and values x and y. The axiom says that if F defines a function on a set d (but doesn't necessarily do so explicitly) then there is a set r containing just those values y corresponding to arguments in d.

Fraenkel and others added this stronger version of the separation principle to Zermelo's axiom set during the 1920s. I don't think it's used in the set theory and logic units. It's required for some constructions in advanced cardinal and ordinal arithmetic. Together with some very simple consequences of the other axioms it implies the separation principle and the axiom of pair sets.

Power set: $\forall z \exists y \forall x (\forall v (v \in x \Rightarrow v \in z) \Rightarrow x \in y)$

This says that for every set z there is a set y containing all subsets $x \subseteq z$.

Given z, apply that axiom to yield y. Use separation with formula P: $\forall v(v \in x \Rightarrow v \in z)$ to obtain s such that $\forall x(x \in s \Leftrightarrow \forall v(v \in x \Rightarrow v \in z))$. By extensionality, s is unique; it's usually denoted by $\mathscr{P}z$.

Pair set: $\forall v \forall w \exists y(v \in y \;\&\; w \in y)$

Given v,w apply that axiom to yield y. Use separation with P: $x = v \vee x = w$ to obtain s such that $\forall x(x \in s \Leftrightarrow (x = v \vee x = w))$. By extensionality, s is unique; it's usually denoted by $\{v,w\}$.

That entails the existence of singletons: $\{w\} = \{w,w\}$ for each w.

Ordered pairs are generally defined by setting $<v,w> = \{\{v\},\{v,w\}\}$.

Union: $\forall S \exists y \forall x \forall z(x \in z \;\&\; z \in S \Rightarrow x \in y)$

Given S, apply that to yield y. Then use separation with P: $\exists z(x \in z \;\&\; z \in S)$ to obtain s such that $\forall x(x \in s \Leftrightarrow \exists z(x \in z \;\&\; z \in S))$. By extensionality, s is unique; it's usually denoted by $\bigcup S$.

This entails existence of $v \cup w = \bigcup\{v,w\}$ for each v,w.

Given a set R, let $y = \bigcup\bigcup R$ and apply separation with formula P: $\exists z(<x,z> \in R)$ to obtain s such that $\forall x(x \in s \Leftrightarrow \exists z(<x,z> \in R))$. By extensionality, s is unique; it's usually denoted by $\operatorname{Dom} R$. You can construct $\operatorname{Rng} R$ similarly.

Given sets V,W let $y = \mathscr{P}\mathscr{P}(V \cup W)$ and apply the separation principle with formula P: $\exists v \exists w(x = <v,w> \;\&\; v \in V \;\&\; w \in W)$ to obtain s such that $\forall x(x \in s \Leftrightarrow \exists v \exists w(x = <v,w> \;\&\; v \in V \;\&\; w \in W)$. By extensionality, s is unique; it's usually denoted by $V \times W$.

You can use separation and extensionality to construct

- converses, because $\breve{R} \subseteq (\operatorname{Rng} R) \times (\operatorname{Dom} R)$ for all R;
- relational products, since $R\,|\,S \subseteq (\operatorname{Dom} R) \times (\operatorname{Rng} S)$;
- identity relations, since $I_V \subseteq V \times V$ for all V;
- relational images, since $R[S] \subseteq \operatorname{Rng} R$;
- Cartesian products, because $X_{S \in \mathcal{S}} S \subseteq \mathscr{P}(\mathcal{S} \times \bigcup\mathcal{S})$.

Choice: $\forall r \exists f(\forall x \forall y \forall y'(<x,y> \in f \;\&\; <x,y'> \in f \Rightarrow y = y')$
$\;\&\; \forall z(z \in f \Rightarrow z \in r) \;\&\; \forall x \forall y(<x,y> \in r \Rightarrow \exists y'(<x,y'> \in f)))$

That's Bernays' form of the axiom: it says that every set r has a subset f that is a function with the same domain. Of course, a formal statement requires rephrasing to replace phrases such as $<x,y'> \in f$ that involve ordered pairs with equivalent phrases that don't, such as

$$\exists a \exists b \exists c(a \in f \;\&\; \forall t(t \in a \Leftrightarrow (t = b \vee t = c)) \;\&\; \forall t(t \in b \Leftrightarrow t = x) \;\&\; \forall t(t \in c \Leftrightarrow (t = x \vee t = y')).$$

Foundation: $\forall y(\exists x(x \in y) \Rightarrow \exists x(x \in y \ \& \ \forall w(w \in x \Rightarrow w \notin y)))$

Often called the *regularity* axiom, this says that every nonempty set y has an element that is disjoint from y. It simplifies the definition of ordinal numbers, and eliminates in one fell swoop some unpleasant possibilities such as sets which belong to each other. Analyzing those tends to be complicated and uninformative. This axiom was added to Zermelo's list during the 1920s. It is not used in the logic and set theory units.

Infinity

The exact form of the axiom of infinity depends on how the natural number system is to be developed. The *Natural Numbers* unit describes different ways of defining "x is a natural number" without postulating any axiom of infinity. That is particularly interesting to those who would investigate a theory of finite sets. It permits use of some features of natural numbers without making assumptions about infinite things.

The axiom is required only when it is necessary to use set theory to manipulate a *set* $\mathbb{N}$ of all natural numbers as in these units. The most direct version of the axiom would say that there is a set y that

- contains the element chosen to represent zero, and
- is closed under the operation chosen to represent construction of the successor of a natural number.

(That operation must satisfy certain requirements.) More formally:

$$\exists y(\exists z(z \text{ represents zero } \& \ z \in y \ \&$$
$$\forall x \forall x^+(x \in y \ \& \ x^+ \text{ represents the successor of } x \Rightarrow x^+ \in y).$$

Once this axiom is applied to yield one such set y, you can define $\mathbb{N}$ to be the intersection of all such sets.

The two most common methods for this construction both choose the empty set to represent zero. Zermelo's technique uses $n^+ = \{n\}$; Neumann's uses $n^+ = n \cup \{n\}$.

The *Natural Numbers* unit shows how to obtain the Peano postulates for the natural number system in the framework of set theory. Many books develop natural number arithmetic from those postulates, using elementary reasoning. Those and others continue, to develop integer, rational, real, and complex arithmetic.