Logic and Mathematics:
Mathematicians in Schools Program

Lashi Bandara
Mathematical Sciences Institute,
Australian National University

April 21, 2011

Contents

1 Russell's Paradox

Sets are at the heart of modern mathematics. The existence of mathematical objects come down to their existence as sets. Sets allow us to conveniently group objects and then to *reason* collectively about them. For instance, $\mathbb{R}$ is the set of real numbers and we can reason that $r_1 + r_2 \in \mathbb{R}$ when $r_1, r_2 \in \mathbb{R}$, which says that the sum of two real numbers are real. The symbol $\in$ is the *belonging* symbol and its use above says that r_1 and r_2 belong to $\mathbb{R}$. We could also consider $\mathbb{N}$, the set of natural numbers and it is not necessarily true that $\frac{n}{m} \in \mathbb{N}$ when $n, m \in \mathbb{N}$. Being a bit more adventurous, one could write $S = \{\text{apple, orange, banana}\}$ which is a set containing an apple, orange and banana and state that everything in S is tasty.

Indulge yourself for a moment and ask yourself the following (philosophical) question: "*what do we mean when we say 'set'?*" Modern mathematicians seek *rigour*, and it is important to characterise and define things that we use. Without rigour, it becomes very easy to make mistakes. An analogy may be to know your tool before you use it. If you don't know how to use a chainsaw properly, you could end up hurting yourself. So, it is important that when we say *set*, we know exactly what this *means.*

Prior to the desire to rigourise, mathematicians were happy to rely entirely upon intuition. Very few considered the importance of this question and *naïvely* assumed that that "*a set is a collection of objects.*" Intuitively, you probably agree with this. As in the construction of the set S above, one should be able to put the brackets $\{\}$ around things and call it a set. Then certainly, there is no obstruction to constructing the set: $\mathscr{U} = \{\text{everything}\}$.

In 1901, Bertrand Russell discovered a most profound blunder. It is probably not an exaggeration to say that it was this discovery which spurred the need for rigour. First, where does the set $\mathscr{U}$ belong? Certainly, since $\mathscr{U}$ contains *everything* we must have $\mathscr{U} \in \mathscr{U}$. So, as bizzarre as it may seem, there were sets that contained themselves! Russell went onto consider the following set:

$$A = \{B \notin B\},$$

where $\notin$ means *does not belong to.* Certainly, there are lots of sets in A. For instance, if we consider the *empty* set $\varnothing = \{\}$, the set that contains *nothing*, then surely we have that $\varnothing \notin \varnothing$ and hence $\varnothing \in A$.

Russell then asked is $A \in A$? Only one of two things can happen: either $A \in A$ or $A \notin A$. Intuitively, either an object belongs somewhere (including itself) or it doesn't. Russell then considered the two cases $A \in A$ and $A \notin A$ separately to understand the consequences.

Suppose that $A \in A$. By the very construction of A, this means we have $A \notin A$. Now suppose that $A \notin A$. Again, by the construction of A, this means that $A \in A$. Since either $A \in A$ or $A \notin A$ must happen, we have that both $A \in A$ and $A \notin A$ are true! This is the infamous *Russell's Paradox.*

Perhaps allowing the absurdity of letting sets contain themselves means we should allow a set to both be contained in itself and not in itself simultaneously. Unfortunately, we will see later that this makes *every* mathematical statement both true and false and thereby renders mathematics useless!

2 Propositional Logic

Mathematical proof, the ability to reason about the truth of a mathematical statement *beyond all doubt*, is central to modern mathematics. This requires a system of logic with which to reason. The most rudimentary system we look at is called *Propositional Logic* for which the basic objects are *propositions.* Propositions are simple sentences to which we can assign either *true* or *false* such as “it is raining” or “the sky is purple.” It is important to emphasise that the logic is one that is *constructed.* This construction is a rigourisation of our intuition.

The basic tool we use to define propositional logic is called a *truth table.* We shall use p and q to stand for arbitrary propositions and T and F to stand for true and false respectively. The first logical operand we construct is called the *negation* or *not.*

Definition 2.1 (Negation)**.** *Negation is denoted by* $\neg$ *and is defined by:*

p	$\neg p$
T	F
F	T

We will now consider how negation interacts with itself. We write it below as a *Proposition* and this is not to be mistaken with “propositions” of Propositional Logic. In this context, Proposition simply means “true statement.” Other name for such true statements are *Lemma* and *Theorem.* Lemmas are usually technical statements (like intermediate steps) that help us prove Propositions and Theorems. The phrase Theorem is usually reserved for a deep and important result. The following result is important, but it is not deep enough to be called a Theorem. It is important to note that the names we choose for our statements are mostly a matter of personal style. Perhaps some mathematician may call the following a Theorem and others a Lemma! Lemmas, Propositions and Theorems are accompanied by proof and we leave the proof of the following as an exercise.

Proposition 2.2. $\neg\neg p = p$.

Next, we want to give meaning to what we mean by p *or* q. Intuitively, this should be true if either p or q or both p and q are true. Also, we consider p *and* q. Here, the only time that this should be true is if only both p and q are true.

Definition 2.3 (Disjunction and Conjunction)**.** *The symbol* $\vee$ *denotes* or *and it is called the* disjunction*. The symbol* $\wedge$ *denotes* and*, and it is called the* conjunction*. We define these by:*

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

We will now consider how negation interacts with conjunction and disjunction. Again, we leave the proof as an exercise.

Proposition 2.4. $\neg(p \vee q) = \neg p \wedge \neg q$ *and* $\neg(p \wedge q) = \neg p \vee \neg q$.

Now we come to perhaps the most important construct of this logic. This is the notion of what it means to say "*if* p *then* q" or p *implies* q.

Definition 2.5 (Implies)**.** *We let* $\implies$ *denote implies and define:*

p	q	$p \implies q$
T	T	T
T	F	F
F	T	T
F	F	T

Certainly $p \implies q$ should be true if both p and q are true and in the case that p is true but q is false, then we should surely want $p \implies q$ to be false. It is the last two lines that are perhaps a point of contention. We will justify it by the following example. Consider the statement "if it rains then it will be wet." We can see the third line in the table by saying that the statement should still be true if it is indeed wet, irrespective of whether it has rained. Lastly, we should expect that "if it is not wet then it cannot have rained" to true whenever the original statement is true. Symbolically, this is exactly requiring that $p \implies q$ is equivalent to $\neg q \implies \neg p$. Substituting $\neg q$ in the place of p and $\neg p$ in the place of q in the truth table above, the first line reads

$\neg q$	$\neg p$	$\neg q \implies \neg p$	p	q
T	T	T	F	F

and this is exactly the last line of the truth table in the definition of implication.

We introduce some terminology. The statement $\neg q \implies \neg p$ is called the *contrapositive* and $q \implies p$ is called the *converse* to the statement $p \implies q$. If $p \implies q$ and $q \implies p$, we say that p and q are *equivalent* or p *if and only if* q and write $p \iff q$.

We have the following useful observation about the implication in terms of the disjunction. In particular, it allows us to compute the negation of an implication. We leave its proof as an exercise.

Proposition 2.6. *We have* $p \implies q = \neg p \vee q = \neg q \implies \neg p$ *and therefore* $\neg(p \implies q) = p \wedge \neg q$.

The negation of the implication gives us an alternative way of defining the implication. Intuitively, the opposite of $p \implies q$ should be true only when p is true but q is false.

Now we come to a grand and remarkable application of the implication to mathematics.

Theorem 2.7. *Let q be any statement and suppose there is a statement p such that both p and $\neg p$ are true. Then, $p \implies q$ is true.*

Proof. We have that $p \implies q = \neg p \vee q$. But since $\neg p$ is true, then $p \implies q$ is true. □

A *Corollary* is an important consequence to a Theorem. Usually, Corollaries are important and immediate observations of Theorems and sometimes are unaccompanied by a proof. The following corollary, however, does deserve some justification.

Corollary 2.8. *Russell's Paradox gives $p = A \in A$ and $\neg p = A \notin A$ being true and therefore every mathematical statement is true.*

3 Predicate Logic

It is essential in mathematics for to be able to reason about collections of objects. Propositional logic lacks the power to *quantify* over general collections. For instance, consider the assertion "the sum of an integer with itself is twice the integer." Propositional logic allows us to write the propositions $1+1 = 2 \times 1$, $2+2 = 2 \times 2$, etc. But what we want to really say is

$$(1+1 = 2 \times 1) \wedge (2+2 = 2 \times 2) \wedge (3+3 = 3 \times 2) \wedge \ldots$$

The "..." are not part of propositional logic and therefore, we must extend the logic in some way.

In propositional logic, we used p and q to denote propositions. Here, we denote *variables* by x, y and *predicates* by $P(x)$ and $Q(x)$. Predicates are *propositional functions.* That is, whenever we substitute x with an actual instance i, then $P(i)$ is a proposition. For instance let $P(x) =$ "x is a mathematician" and by setting $x =$ "Cantor" yields the proposition $p = P($"Cantor"$) =$ "Cantor is a mathematician".

We shall proceed to define predicate logic in a more intuitive way than that is typically done in logic where it is defined rather formally through a set of axioms. This is because we are really interested in rigourising our intuition in order to do mathematics and we can lose sight of intuition if we are overly formal.

The first quantifier we introduce is the *existential* quantifier.

Definition 3.1 (Existential quantifier)**.** *Let $\exists$ denote the existential quantifier and we define:*

$$\exists x P(x) = \begin{cases} T & \textit{if there is a } x_0 \textit{ that makes } P(x_0) \textit{ true} \\ F & \textit{otherwise} \end{cases}.$$

The existential quantifier captures the notion of "there exists some x such that $P(x)$ is true." For example, let us consider the predicate $P(x) =$ "x is irrational" (of course, one needs to first define what it means for a number to be irrational). There are two important philosophical points here that are worth a mention. First, this is different to the proposition $p =$ "π is irrational" although it is true that $p \implies \exists x P(x)$. In some sense, the statement $\exists x P(x)$ is *weaker* than p because it lends itself to the possibility that one can prove it *without* having to produce an actual such number. There may be instances where the actual irrational number may not be important, but the fact that such a number exists is. We remark that often in writing mathematical proofs, we use the words "there exists" in place of $\exists$.

The other quantifier that we define is the *universal* quantifier.

Definition 3.2 (Universal quantifier)**.** *We let $\forall$ denote the universal quantifier and define $\forall x P(x) = \neg \exists x \neg P(x)$.*

The definition here reads that $\forall x P(x)$ is true if "there *does not* exist an x that makes $P(x)$ false." That is, "for all x we have that $P(x)$ is true." Let the predicate $P(x)$ be

$x + x = 2x$. Then, $\forall x[x \in \mathbb{Z} \implies P(x)]$ encapsulates the "..." of our first example. Often, when we have some collection A, the shorthand notation $\forall x \in A\ [P(x)]$ is the same as $\forall x[x \in A \implies P(x)]$. As we saw with the existential quantifier, we often write out in words "for all $x \in A$ we have $P(x)$" in place of the symbolic notation.

We also point out that we implicitly used predicates and both these quantifiers prior to their definition here. Consider Theorem 2.7 and its Corollary 2.8. In the Theorem, we let "*...q be any statement...*" which is universal quantification over propositions, and "*...suppose there is a statement p such that...*" which is exactly an existential quantification. It is only now that these two statements stand justified in logic.

The following proposition outlines some of the important properties of predicate logic.

Proposition 3.3. *(i)* $\neg\neg P(x) = P(x)$,

(ii) $\neg(P(x) \wedge Q(x)) = \neg P(x) \vee \neg Q(x)$,

(iii) $\neg(P(x) \vee Q(x)) = \neg P(x) \wedge \neg Q(x)$,

(iv) $P(x) \implies Q(x) = \neg P(x) \vee Q(x)$,

(v) $P(x) \implies Q(x) = \neg Q(x) \implies \neg P(x)$,

(vi) $\forall x \neg P(x) = \neg \exists x P(x)$,

(vii) $\exists x P(x) = \neg \forall x \neg P(x)$.

Proof. For (i), fix x, so that $p = P(x)$ is a proposition. Then by Proposition 2.2, we have $\neg\neg P(x) = \neg\neg p = p = P(x)$. We leave the rest as an exercise. □

Often, mathematical statements use a combination of the two quantifiers. The order in which they are used is very important. Consider the difference between the sentences "somebody loves everybody" and "everybody is loved by somebody." The first sentence says that some person loves every person. The second says that given a person, there is some person that loves them. Thus, in the second, the person giving the love may change from one person to the next. We can encapsulate this in predicate logic. Let $P(x, y) =$ "x is loved by y". Then, the first sentence is given by $\exists y \forall x P(x, y)$ whereas the second is give by $\forall x \exists y P(x, y)$.

Lastly, we highlight a little curiosity known as *vacuous truth*; anything you say about nonexistent objects are true.

Proposition 3.4. *Let $P(x)$ be a predicate. Then, $\forall x \in \varnothing\ [P(x)]$.*

Proof. We note that $\forall x \in \varnothing\ [P(x)]$ is exactly $\forall x[x \in \varnothing \implies P(x)]$. Now, by Proposition 3.3, $x \in \varnothing \implies P(x) = x \notin \varnothing \vee P(x)$ and this is always true since $\varnothing = \{\}$. □

In particular, "all pink elephants can fly" and "all earth sized rhinos are elephants" are true!

4 Counting

Counting, undoubtedly, is one of the most fundamental aspects of mathematics. We can identify 3 bananas or 5 apples, but what exactly does this actually mean? In fact, is it even sensible to say 3 or 5? Here, we answer the latter question in the positive by an abstract construction of numbers. Consequently, with the aid of some additional machinery, we settle the former question.

First, we recall some notions regarding sets but we phrase them precisely in the language of predicate logic.

Definition 4.1 (Operations on Sets)**.** *Let A and B be sets. We define:*

(i) $A \cup B = \{x : x \in A \vee x \in B\}$ *(Union),*

(ii) $A \cap B = \{x : x \in A \wedge x \in B\}$ *(Intersection),*

(iii) $A = B$ *if* $x \in A \iff x \in B$ *(Equality),*

(iv) $A \subset B$ *if* $x \in A \implies x \in B$ *(Subset),*

(v) $A \subsetneq B$ *if* $A \subset B$ *and* $A \neq B$ *(Strict Subset).*

We construct the natural numbers *inductively.* That is, the construction of the n^{th} number will depend on the numbers constructed before it. It is worth noting that we include 0 as a natural number. There is little debate whether this is the right thing to do since it is a matter of taste and convenience.

Definition 4.2 (Natural numbers)**.** *Let*

$$0 = \varnothing, \quad 1 = \{0\}, \quad 2 = \{0, 1\} \quad 3 = \{0, 1, 2\},$$

and so on. That is, for a number n, let $N(n)$ denote the number immediately after n and then,

$$N(n) = \{0, \dots, n\}.$$

We let $\mathbb{N} = \{0, 1, 2, \dots\}$ *which is the set of natural numbers.*

This construction imposes the following natural ordering on $\mathbb{N}$.

Definition 4.3 (Ordering of $\mathbb{N}$)**.** *Let $m, n \in \mathbb{N}$. If $m \subset n$, we write $m \leq n$ and say that m is less than n. If $m \subsetneq n$, then we write $m < n$ and say that m is strictly less than n.*

We leave the proof of the following observations as an exercise.

Proposition 4.4. *(i) If $l < m$ and $m < n$, then $l < n$ (and similarly for $\leq$ in place of $<$),*

(ii) If $m \leq n$ and $n \leq m$ then $m = n$.

In particular, if $m \neq n$, then either $m < n$ or $n < m$ (and not both).

Our construction yields a rigorous notion of number that is *abstract.* That is, the numbers themselves are objects and we can say 3 rather than having to say 3 of something. But now, suppose we are just given a set A of apples. What does it mean to say that A contains n things? Intuitively, if we can set up a *correspondence* with the number n with elements of A, then this certainly seems a reasonable way to count. To achieve this purpose, we define the notion of a *function* rigorously in logic. Throughout this section, we let A, B, and C denote sets.

Definition 4.5 (Function)**.** *Let $F \subset A \times B = \{(a,b) : a \in A,\ b \in B\}$ such that for each $a \in A$, there is a $b \in B$ such that $(a,b) \in F$. If $(a,b),\ (a,c) \in F \implies b = c$, the we say that F is a function (or map) $f : A \to B$ defined by $f(a) = b$ whenever $(a,b) \in F$. The range of a function is then $\mathcal{R}(f) = \{a \in A : f(a)\} \subset B$.*

A function encapsulates the notion of something that takes an input and spits out a *single* output. The definition here says that we *do not* have an $a \in A$ such that $f(a) = b$ and $f(a) = c$ with $b \neq c$. Also, note that $F = \{(a, f(a)) : a \in A\}$. The following types of functions will be useful to us.

Definition 4.6 (Injective, Surjective, Bijective)**.** *Suppose $f : A \to B$ is a function. We say that f is*

(i) Injective (one to one) if for all $a, b \in A$ we have $f(a) = f(b) \implies a = b$,

(ii) Surjective (onto) if for every $b \in B$, there exists an $a \in A$ such that $f(a) = b$,

(iii) Bijective if it is injective and surjective.

Let us take some time to dismantle and understand these definitions. The definition of an injective function says exactly that we cannot have two elements $a, b \in A$ mapping to the same element under f. Surjectivity tells us that the range of the function is the entire set B. Thus, the notion of bijectivity gives us a notion of correspondence - for every element in B, there is some element in A *and* no two elements in A are mapped to the same element in B. We now have enough technology to define the notion of *cardinality* which encapsulates the number of elements in a set.

Definition 4.7 (Cardinality)**.** *We say that* $\operatorname{card} A = n$ *for some natural number n if there exists a bijection $f : A \to n$.*

To explore this notion further, and in particular to ask whether this is a *good* notion of counting, we require some further terminology.

Definition 4.8 (Composition of functions)**.** *Suppose that $f : A \to B$ and $g : B \to C$ are functions. Then we define the function $g \circ f : A \to C$ by $(g \circ f)(x) = g(f(x))$.*

Definition 4.9 (Identity)**.** *The map $\mathrm{id}_A : A \to A$ defined by $\mathrm{id}_A(x) = x$ for $x \in A$ is called the identity function.*

With this terminology in mind, we make an important observation about bijective functions. We leave its proof as an exercise.

Proposition 4.10. *A function $f : A \to B$ is bijective if and only if there exists a map $g : B \to A$ such that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$.*

Definition 4.11 (Inverse)**.** *The the map g in Proposition 4.10 is called the inverse of f and it is denoted by $f^{-1} = g$.*

Corollary 4.12. *The inverse is a bijection.*

Now, we consider the way these three notions behave under composition.

Proposition 4.13. *Let A, B, C be sets and let $f : A \to B$ and $g : B \to C$. Then:*

(i) if f, g are injective, then so is $g \circ f$,

(ii) if f, g are surjective, then so is $g \circ f$,

(iii) if f, g are bijective, then so is $g \circ f$.

Proof. We prove (i). Fix $a, b \in A$. Then $f(a), f(b) \in B$. By the injectivity of g, we get that $g(x) = g(y) \implies x = y$ for any $x, y \in B$. So, setting $x = f(a)$ and $y = f(b)$ we get that $f(a) = f(b)$. Then, invoking the injectivity of f, we get that $a = b$. Therefore, $g \circ f$ is injective. We leave the rest as an exercise. □

We end this section by pointing out the following crucial observation which reinforces our intuition about counting.

Theorem 4.14. *We have that* $\operatorname{card} A = \operatorname{card} B$ *if and only if there exists a bijection between A and B.*

Proof. Suppose $\operatorname{card} A = \operatorname{card} B = n$. So, there exist bijections $f : A \to n$ and $g : B \to n$. But by Proposition 4.10, we can find a bijection $g^{-1} : B \to n$. Then, invoking (iii) of Proposition 4.13, we get that $g^{-1} \circ f : A \to B$ is a bijection.

For the reverse direction, suppose there exists a bijection $h : A \to B$. Then, again by Proposition 4.10, we get a bijection $h^{-1} : B \to A$. Suppose now that $\operatorname{card} A = m$ and $\operatorname{card} B = n$ and that $f : A \to m$ and $g : B \to n$ are bijections. Again, invoking (iii) of Proposition 4.13, but $g \circ h : A \to n$ and $f \circ h^{-1} : B \to m$ are bijections. This is exactly that $\operatorname{card} B = m$ and $\operatorname{card} A = n$. Therefore, $m = n$ and the proof is complete. □

This theorem reveals that our notion of counting is *well defined.* That is, if we have a different number of elements in A to B, then there should be no correspondence between them.

5 Infinity

We intuitively understand that when we say "infinity," we mean something that is forever or boundless. But what does this exactly mean? Since we have a notion of being able to count finite sets, we can use this notion to define what we mean by *infinity*. Throughout this section, we let A, B, C be sets.

Definition 5.1 (Finite and Infinite)**.** *We say that a set A is finite if there exists an $n \in \mathbb{N}$ and there exists a bijection $f : A \to n$. We say that A is infinite if it is not finite.*

We explore this notion of infinity further by using the machinery we have previously constructed around injective, surjective and bijective functions. It is worth emphasising that most of this machinery works for arbitrary sets. In fact, the only time we alluded to finiteness was when we were dealing with finite cardinality. First, we will characterise our notion of infinity more directly.

Proposition 5.2. *A is infinite if for every number n and for every function $f : A \to n$ we have that f is not a bijection.*

Proof. Write out the definition of finite formally and then take the negation. We leave this as an exercise. □

In mathematics, it is always important to establish the *existence* of objects that satisfy notions that we define. This is because by vacuous truth, if there are no objects that satisfy the notion, then anything we say about such objects are true. In this context, existence translates to the following question: does there exist an infinite set? We need to develop some more machinery to purse this question.

Proposition 5.3. *Let $f : A \to B$ be injective. Let $f(A) = \{f(a) : a \in A\} = \mathcal{R}(f)$. Then, $f : A \to f(A)$ is bijective.*

Proof. We already have that f is injective, and surely, it is surjective to its own image. That is, take any $b \in f(A)$. By definition of $f(A)$, there exists an $a \in A$ such that $b = f(a)$. □

We note a subtlety and an abuse of notation here. We have called both these functions f, but in fact, the second function is restricted to its range. This is indeed a different function and hence why we write $f : A \to f(A)$ rather than simply f.

Proposition 5.4. *Let $f : A \to B$ be a function. If f is a bijection then for any subset $C \subset A$, the restricted map $f|_C : C \to f(C)$ is a bijection.*

We leave the proof as an exercise and note the following important Corollary.

Corollary 5.5. *If there exists a $C \subset A$ such that $f|_C : C \to f(C)$ is not a bijection, then $f : A \to B$ is not a bijection.*

Now, we meet our first infinite set.

Theorem 5.6. *The set $\mathbb{N}$ is infinite.*

Proof. We prove by contradiction. That is, assume that $\mathbb{N}$ is finite. Therefore, there exists an $m \in \mathbb{N}$ and $f : \mathbb{N} \to m$ a bijection. Let $N(m) = \{0, 1, \ldots, m\}$ denote the number right after m. Then, $N(m) \subset \mathbb{N}$ and furthermore $N(m) > m$. By Theorem 4.14 and Proposition 4.4 there cannot be any bijection $g : N(m) \to g(N(m))$ but by Proposition 5.4, $f|_{N(m)} : N(m) \to f(N(m))$ is a bijection and we draw a contradiction. □

We note here that we have been informal and logically blasé about the nature of proof by contradiction. We could in fact prove this in logic. We state this precisely and leave this as an exercise.

Proposition 5.7 (Proof by contradiction)**.** *Let P, Q be predicates and suppose that $P \implies Q$ is true but Q is false. Then, $\neg P$ is true.*

Now, consider Theorem 4.14. This theorem says exactly that two finite sets contain the same number of elements if there exists a bijection between them. There is no reason why we cannot apply this notion to infinite sets. In fact, here, we extend the term *cardinality* to all sets, and talk about arbitrary (even infinite) sets having the same cardinality to mean that they contain the same "number" of things. This idea is somewhat abstract, but we have little choice but to rely upon the machinery we have for the finite setting and generalise to the infinite setting.

Definition 5.8 (Cardinality)**.** *If there exists $f : A \to B$ a bijection, then we say that the two sets have the same number of elements and write* $\operatorname{card} A = \operatorname{card} B$.

We remark and emphasise here that unlike in the finite world where we could explicitly define $\operatorname{card} A$ to be a number, in the arbitrary setting, we do not have the luxury of an "infinite number." To labour the point, we can only talk about $\operatorname{card} A = \operatorname{card} B$ meaning that the two sets A and B have the same "number" of things, without alluding to what this "number" actually is! It is also worth noting at this point whether this definition is at all necessary. Is there more than one infinity? Our intuition tells us that infinity is something boundless but is it obvious that all things boundless are bijective to each other?

As a first step in answering these questions, we have the following non-intuitive result regarding infinite sets. Note that by Proposition 4.4, such a result is *impossible* for finite sets!

Theorem 5.9. *Let $\mathscr{E} = \{2, 4, 6, 8, \ldots\} = \{2n : n \in \mathbb{N}\} \subsetneq \mathbb{N}$ be the set of even numbers. Then, there exist a bijection $f : \mathbb{N} \to \mathscr{E}$.*

Proof. Let $f : \mathbb{N} \to \mathscr{E}$ be defined by $f(n) = 2n$. We leave it as an exercise to prove that f is a bijection. □

This Theorem tells us something quite remarkable. It says that when a set is infinite, it is possible to have a bijection with a proper subset of itself. Indeed, this result tempts us in the direction that perhaps all infinities are equally as "large." But to try attempt to rigorously pursue this question, we need a notion of *order* for infinite sets.

Definition 5.10 (Order)**.** *Suppose that* $f : A \to B$ *is an injection. Then, we say that* $\operatorname{card} A \leq \operatorname{card} B$. *If further there does not exist a bijection* $g : A \to B$*, then we write* $\operatorname{card} A < \operatorname{card} B$.

Is this notion of order actually well defined? In this context, it means whether it generalises our notion of order for finite sets. We can indeed show that this is a well defined notion by the following proposition. We leave its proof as an exercise.

Proposition 5.11. *Suppose that* A, B *are finite. Then,* $\operatorname{card} A \leq \operatorname{card} B$ *if and only if there exists an injection* $f : A \to B$. *Similarly,* $\operatorname{card} A < \operatorname{card} B$ *if and only if* $\operatorname{card} A \leq \operatorname{card} B$ *and there does not exist a bijection* $f : A \to B$.

We require the following notion of a *Power set* which, intuitively, given any set, associates a very large set to it.

Definition 5.12 (Powerset)**.** *We define the powerset of* A *to be* $\mathscr{P}(A) = \{X : X \subset A\}$*, the collection of all subsets of* A.

For a moment, let us consider the power set of A when A is finite. It is easy to verify then that $\operatorname{card} A < \operatorname{card} \mathscr{P}(A)$. To be informal and intuitive, if the set A has n elements, then its powerset has 2^n elements, so the power set grows exponentially. The intuition we gain in this finite setting has a remarkable generalisation to the infinite in the form of the following theorem.

Theorem 5.13 (Cantor's Theorem)**.** *For any set* A*, we have that* $\operatorname{card} A < \operatorname{card} \mathscr{P}(A)$.

Proof. First, we show that $\operatorname{card} A \leq \operatorname{card} \mathscr{P}(A)$. Define $f : A \to \mathscr{P}(A)$ by $f(x) = \{x\} \subset A$. Now, suppose that $f(x) = f(y)$. This is exactly $\{x\} = \{y\}$ so $x = y$. This proves that f is an injection.

We prove now that there cannot exist a bijection $g : A \to \mathscr{P}(A)$. To derive a contradiction, suppose such a bijection does exist. So, for each $x \in A$, $g(x) \subset A$. Define $B = \{x \in A : x \notin g(x)\}$. Since $g(x)$ is a bijection, in particular it is a surjection and there exists some $y \in A$ such that $g(y) = B$. But note now that if $y \in B$, then by construction, $y \notin g(y) = B$. If $y \notin B = g(y)$, then by construction of B, $y \in B$. Thus we have a contradiction and so conclude that there cannot exist a bijection between A and $\mathscr{P}(A)$. □

This is deep and nontrivial. Its power is astounding: it tells us that there is an "infinity" of infinities. By taking power sets successively, we get larger and larger infinities! In particular, it answers our question about the nature of infinity: infinity is not simply a single object but there are "infinity" many of them.