Some Comments on Infinite Sets

David E. Radford 11/19/05 (slight corrections 11/21/05)

Suppose that A is an infinite set. Constructing a denumerable subset $\{a_1, a_2, a_3, \ldots\}$ of A, which is the same as showing that there is an injection $f : \mathbf{Z}^+ \longrightarrow A$, requires more than just mathematical induction. In these notes we explore some consequences of basic definitions con cerning infinite sets with the aid of mathematical induction only. We show that the set of rational numbers, and more generally the set of real algebraic numbers, is denumerable.

These notes supplement part of the discussion of infinite sets in the text.

1 Counting and Equipotent Sets

Counting the elements of a non-empty finite set A boils done to labelling the elements by $1, 2, 3, \ldots, n$ for some $n \geq 1$. This is tantamount to defining a bijection $f : \{1, 2, 3, \ldots, n\} \longrightarrow A$. Evidently finite sets A and B have the same number of elements if and only if there is a bijection $f : A \longrightarrow B$.

Now suppose that A, B, and C are *any* non-empty sets. Then A and B are *equipotent* if there is a bijection $f : A \longrightarrow B$, in which case we write $A \sim B$. Since the identity map $I : A \longrightarrow A$ is bijective,

$$A \sim A.$$

Suppose that $A \sim B$. Then there is a bijection $f : A \longrightarrow B$. Since $f^{-1} : B \longrightarrow A$ is also a bijection, we have

$$A \sim B \qquad \text{implies} \qquad B \sim A.$$

Suppose that $A \sim B$ and $B \sim C$. Then there are bijections $f : A \longrightarrow B$ and $g : B \longrightarrow C$. Since the composition $g \circ f : A \longrightarrow C$ is a bijection, we have shown

$$A \sim B \quad \text{and} \quad B \sim C \qquad \text{implies} \quad A \sim C.$$

In other words, equipotent defines an equivalent relation on any non-empty collection of non-empty sets. See Chapter 22 of the text.

2 Finite Sets and Denumerable Sets

Let A be a set. Then A is *finite* if $A = \emptyset$ or if there is a bijection $f : \mathbf{N}_n \longrightarrow A$ for some $n \geq 1$, where

$$\mathbf{N}_n = \{1, 2, 3, \ldots, n\}.$$

Sets which are not finite are called *infinite*. An infinite set A is *denumerable* if there is a bijection $f : \mathbf{Z}^+ \longrightarrow A$, where

$$\mathbf{Z}^+ = \{1, 2, 3, \ldots\}.$$

A set which is either finite or denumerable is said to be *countable*. A fundamental example of an infinite set is $\mathbf{Z}^+$.

Suppose that A is denumerable. Then there is a bijection $f : \mathbf{Z}^+ \longrightarrow A$ by definition. Set $a_n = f(n)$ for all $n \geq 1$. Then

$$A = \{a_1, a_2, a_3, \ldots\} \qquad \text{and} \qquad a_m = a_n \text{ implies } m = n. \tag{1}$$

The first assertion follows since f is surjective and the second since f is injective.

Here are a few examples of denumerable sets.

Example 1 *The set of all positive integers* $\mathbf{Z}^+$*.*

This follows since the identity map $I : \mathbf{Z}^+ \longrightarrow \mathbf{Z}^+$ is a bijection.

Example 2 *The set of all non-negative integers* $\mathbf{Z}^{\geq}$*.*

To see this we note that the function $f : \mathbf{Z}^+ \longrightarrow \mathbf{Z}^{\geq}$ defined by $f(n) = n - 1$ is a bijection.

To continue, we observe that every integer n is either even or odd, and not both. If n is even then $n = 2m$ for one and only one integer m. Likewise, if n is odd, then $n = 2m + 1$ for one and only one integer m. As $2m + 1 = 2(m + 1) - 1$, every odd integer n can be written $n = 2m - 1$ for one and only one integer m also.

Example 3 *The set A of all positive* even *integers.*

To see this we note that the map $f : \mathbf{Z}^+ \longrightarrow A$ defined by $f(n) = 2n$ for all $n \geq 1$ is a bijection.

Example 4 *The set A of all positive* odd *integers.*

To see this we note that the map $f : \mathbf{Z}^+ \longrightarrow A$ defined by $f(n) = 2(n-1)+1 = 2n-1$ for all $n \geq 1$ is a bijection.

Example 5 *The set of all integers* $\mathbf{Z}$.

To see this we note that the map $f : \mathbf{Z}^+ \longrightarrow \mathbf{Z}$ defined by

$$f(n) = \left\{ \begin{array}{rcl} m & : & n \text{ even, } n = 2m; \\ -m & : & n \text{ odd, } n = 2m+1 \end{array} \right.$$

is a bijection.

The following proposition will enable us to describe less obvious examples of denumerable sets rather easily.

Proposition 1 *Let A be a denumerable set and let B be an infinite set. Then B is denumerable if either*

a) *there is an injection $f : B \longrightarrow A$*

or

b) *there is a surjection $f : A \longrightarrow B$.*

Proof: Write $A = \{a_1, a_2, a_3, \ldots\}$ as in (1). We first show part a) implies part b).

Suppose that $f : A \longrightarrow B$ is a surjection. We will construct an injection $g : B \longrightarrow \mathbf{Z}^+$. Since $\mathbf{Z}^+$ is denumerable by Example 1, this will be enough to show that part a) implies part b).

Since f is surjective, we can write $B = \{b_1, b_2, b_3, \ldots\}$, where $b_n = f(a_n)$ for all $n \geq 1$. Since f is not necessarily injective, there may be duplications in the list of elements of B.

We define a function $g : B \longrightarrow \mathbf{Z}^+$ as follows. Let $b \in B$. Then $b = b_m = f(a_m)$ for some $m \geq 1$. Let $S = \{\ell \in \mathbf{Z}^+ \,|\, b = b_\ell\}$. Then S is a subset of positive integers which is not empty since $m \in S$. Therefore S has a (unique) least element n. Set $g(b) = n$. Then $b = b_n = f(a_n)$. In particular $g(b) = n$ implies $b = f(a_n)$.

The function g is an injection. Suppose that $b, b' \in B$ and $g(b) = g(b')$. Set $n = g(b)$. Then $n = g(b')$ also since $g(b) = g(b')$. Consequently $b = f(a_n)$

and $b' = f(a_n)$ which means $b = b'$. We have shown g is an injection. Therefore part a) implies part b).

It remains to show part a). Suppose that $f : B \longrightarrow A$ is an injection. Then $f^+ : B \longrightarrow \operatorname{Im} f$ is a bijection. To show part a), we need only construct a bijection $g : \operatorname{Im} f \longrightarrow \mathbf{Z}^+$. For then $(f^+)^{-1} \circ g^{-1} : \mathbf{Z}^+ \longrightarrow B$ is a bijection and thus B is denumerable by definition.

Now $\operatorname{Im} f$ is infinite since B is and f^+ is a bijection. Thus the existence of a bijection $g : \operatorname{Im} f \longrightarrow \mathbf{Z}^+$ will follow from:

$$\text{If } B \subseteq A \text{ is infinite, there is a bijection } h : B \longrightarrow \mathbf{Z}^+. \tag{2}$$

To construct h we do the following. We run through the list $a_1, a_2, a_3, \ldots$ of elements of A crossing out the items which are not in B. What remains is a listing of the elements of B. For $b = a_n \in B$ let $h(b)$ be the position of b in this listing of the elements of B. Thus

$$h(b) = |\{m \in \mathbf{Z}^+ \,|\, 1 \leq m \leq n, a_m \in B\}|.$$

Note that h is *well-defined*. Suppose that $b = a_{n'}$ also, where $n' \in \mathbf{Z}^+$. Then $a_n = a_{n'}$ and thus $n = n'$ by (1).

We first show that h is an injection. Suppose that $b, b' \in B$ satisfy $b \neq b'$. Now $b = a_n$ and $b' = a_{n'}$ for some $n, n' \in \mathbf{Z}^+$. Since $b \neq b'$ necessarily $n \neq n'$. Without loss of generality we may assume $n < n'$. Observe that

$$\{m \in \mathbf{Z}^+ \,|\, 1 \leq m \leq n, a_m \in B\} \subset \{m \in \mathbf{Z}^+ \,|\, 1 \leq m \leq n', a_m \in B\};$$

containment follows since $n \leq n'$ and inequality follows since n' belongs to the second set but not the first. Therefore

$$|\{m \in \mathbf{Z}^+ \,|\, 1 \leq m \leq n, a_m \in B\}| < |\{m \in \mathbf{Z}^+ \,|\, 1 \leq m \leq n', a_m \in B\}|,$$

or $h(b) < h(b')$. We have shown that $b \neq b'$ implies $h(b) \neq h(b')$. Therefore h is an injection.

The last detail of the proof of part a), and thus of the proof of the proposition, is to show that h is a surjection. This we do by induction; we show that all $n \in \mathbf{Z}^+$ are images.

First of all $h(b) = 1$ for some $b \in B$. To show this we note that B is not empty since B is infinite. Choose a $b' \in B$. Then $b' = a_{n'}$ for some $n' \in \mathbf{Z}^+$. Let $S = \{\ell \in \mathbf{Z}^+ \,|\, a_\ell \in B\}$. Then S is a subset of positive integers which is not empty since $n' \in S$. Thus S has a (unique) least element n. Let $b = a_n$. Then

$$\{m \in \mathbf{Z}^+ \,|\, 1 \leq m \leq n, a_m \in B\} = \{n\}$$

which implies $h(b) = 1$.

Suppose that $n \geq 1$ and $h(b) = n$ for some $b \in B$. We will show that $h(b') = n + 1$ for some $b' \in B$.

We may write $b = a_{n'}$ for some $n' \geq 1$. Thus

$$n = h(b) = |\{m \in \mathbf{Z}^+ \,|\, 1 \leq m \leq n', a_m \in B\}|$$

by definition. Consider the subset of positive integers $S = \{m \in \mathbf{Z}^+ \,|\, n' < m, a_m \in B\}$. Since B is infinite, $S \neq \emptyset$. Therefore S has a (unique) least element n''. As a consequence if $n' < \ell < n''$ then $a_\ell \notin B$. As $a_{n''} \in B$ we now conclude that

$$\{m \in \mathbf{Z}^+ \,|\, 1 \leq m \leq n'', a_m \in B\} = \{m \in \mathbf{Z}^+ \,|\, 1 \leq m \leq n', a_m \in B\} \cup \{n''\}.$$

Observe the union is disjoint. Let $b' = a_{n''}$. Then

$$\begin{aligned} h(b') &= |\{m \in \mathbf{Z}^+ \,|\, 1 \leq m \leq n'', a_m \in B\}| \\ &= |\{m \in \mathbf{Z}^+ \,|\, 1 \leq m \leq n', a_m \in B\} \cup \{n''\}| \\ &= |\{m \in \mathbf{Z}^+ \,|\, 1 \leq m \leq n', a_m \in B\}| + 1 \\ &= h(b) + 1 \\ &= n + 1. \end{aligned}$$

We have shown $h(b') = n + 1$. Thus by induction for all $n \geq 1$ there is a $b \in B$ such that $h(b) = n$; that is h is surjective. □

3 Some Immediate Applications of the Proposition

Examples 3 and 4 are explained by:

Corollary 1 *Infinite subsets of denumerable sets are denumerable.*

Proof: Let A be a denumerable set and suppose that B is an infinite subset of A. The function $f : B \longrightarrow A$ defined by $f(b) = b$ for all $b \in B$ is an injection. Therefore the corollary follows Proposition 1. □

Corollary 2 *Suppose that $A_1, \ldots, A_n$ are countable sets and at least one of them is denumerable. Then $A_1 \cup \cdots \cup A_n$ is denumerable.*

PROOF: We may assume the sets are not empty. Once the case of $n = 2$ is established, the corollary can be proved by induction on n. Suppose that $n = 2$ and write $A = A_1$ and $B = A_2$. Since $B \cup A = A \cup B$ we may assume that A is denumerable.

By (1) we can write $A = \{a_1, a_2, a_3, \ldots\}$. If B is denumerable then we can write $B = \{b_1, b_2, b_3, \ldots\}$ as well. Suppose that B is finite. Then $B = \{b_1, b_2, b_3, \ldots, b_n\}$ for some $n \geq 1$. In this case define $b_m = b_n$ for all $m > n$. Then $B = \{b_1, b_2, b_3, \ldots\}$.

Define $f : \mathbf{Z}^+ \longrightarrow A \cup B$ by

$$f(n) = \begin{cases} a_m & : \; n \text{ even, } n = 2m; \\ b_m & : \; n \text{ odd, } n = 2m - 1. \end{cases}$$

The reader is left with the small exercise of showing that f is a surjection. Since A is infinite and $A \subseteq A \cup B$, it follows that $A \cup B$ is infinite. Since $\mathbf{Z}^+$ is denumerable, $A \cup B$ is denumerable by Proposition 1. □

The proof of our next corollary is built around the infinite subset

$$\mathcal{Z}^+ = \{2^m 3^n \mid m, n \in \mathbf{Z}^+\}$$

of $\mathbf{Z}^+$. By Corollary 1 it follows that $\mathcal{Z}^+$ is denumerable.

Suppose that $2^m 3^n = 2^{m'} 3^{n'}$, where $m, n, m', n' \in \mathbf{Z}^+$. We will show that $m = m'$ and $n = n'$.

Without loss of generality we may assume $m \leq m'$. Therefore $3^n = 2^{m'-m} 3^{n'}$. Now 3^m is an odd integer, and $2^{m'-m} 3^{n'}$ is an even integer unless $2^{m'-m} = 1$, or equivalently $m = m'$. Therefore $m = m'$ which implies $3^n = 3^{n'}$, or equivalently $n = n'$.

Corollary 3 *Suppose that $A_1, \ldots, A_n$ are non-empty countable sets and at least one of them is denumerable. Then $A_1 \times \cdots \times A_n$ is denumerable.*

PROOF: Once the case of $n = 2$ is established, the corollary can be proved by induction on n. Suppose $n = 2$ and set $A = A_1, B = A_2$. By virtue of the proof of the preceding corollary we may write $A = \{a_1, a_2, a_3, \ldots\}$ and

$B = \{b_1, b_2, b_3, \ldots\}$. Since one of A and B is denumerable, and the other is non-empty, $A{\times}B$ is infinite. Define $f : \mathcal{Z}^+ \longrightarrow A{\times}B$ by

$$f(2^m 3^n) = (a_m, b_n)$$

for all $m, n \in \mathbf{Z}+$. Note that f is well-defined. For if $2^m 3^n = 2^{m'} 3^{n'}$, where $m, n, m', n' \in \mathbf{Z}^+$, we have shown that $m = m'$ and $n = n'$. Thus $(a_m, b_n) = (a_{m'}, b_{n'})$. Since $\mathcal{Z}^+$ is denumerable, $A{\times}B$ is infinite, and f is a surjection, $A{\times}B$ is denumerable by Proposition 1. □

Corollary 4 *The set* $\mathbf{Q}$ *of rational numbers is denumerable.*

Proof: By Examples 5 and 1 the set of integers $\mathbf{Z}$ and the set of positive integers $\mathbf{Z}^+$ are denumerable. By Corollary 3 the Cartesian product $\mathbf{Z}{\times}\mathbf{Z}^+$ is denumerable. Now $\mathbf{Q}$ is infinite, since the infinite set $\mathbf{Z}^+ \subseteq \mathbf{Q}$, and the function $f : \mathbf{Z}{\times}\mathbf{Z}^+ \longrightarrow \mathbf{Q}$ defined by $f((m, n)) = m/n$ is a surjection. Therefore $\mathbf{Q}$ is denumerable by Proposition 1. □

4 Unions and Intersections of Families of Sets, Algebraic Numbers

Suppose that I is a non-empty set and $\{A_\imath\}_{\imath \in I}$ is family of sets indexed by the set I. Then the union and intersection of the family are defined by

$$\bigcup\nolimits_{\imath \in I} A_\imath = \{a \mid \exists \imath \in I, a \in A_\imath\}$$

and

$$\bigcap\nolimits_{\imath \in I} A_\imath = \{a \mid \forall \imath \in I, a \in A_\imath\}.$$

When $I = \{1, 2, \ldots, n\}$ these definitions agree with the inductive definitions of $A_1 \cup \cdots \cup A_n$ and $A_1 \cap \cdots \cap A_n$.

De Morgan's Laws hold for indexed families of sets. Suppose that U is a universal set and $A_\imath \subseteq U$ for all $\imath \in I$. Then it is easy to see that

$$\bigcup\nolimits_{\imath \in I} A_\imath = \{a \in U \mid \exists \imath \in I, a \in A_\imath\}$$

and

$$\bigcap\nolimits_{\imath \in I} A_\imath = \{a \in U \mid \forall \imath \in I, a \in A_\imath\}.$$

Therefore

$$(\bigcup_{\imath\in I}A_\imath)^c = \{a \in U \,|\, \text{not}(\exists \imath \in I, a \in A_\imath)\} = \{a \in U \,|\, \forall \imath \in I, \text{not}(a \in A_\imath)\} = \bigcap_{\imath\in I}A_\imath^c$$

and

$$(\bigcap_{\imath\in I}A_\imath)^c = \{a \in U \,|\, \text{not}(\forall \imath \in I, a \in A_\imath)\} = \{a \in U \,|\, \exists \imath \in I, \text{not}(a \in A_\imath)\} = \bigcup_{\imath\in I}A_\imath^c$$

from which we conclude

$$(\bigcup_{\imath\in I}A_\imath)^c = \bigcap_{\imath\in I}A_\imath^c \quad \text{and} \quad (\bigcap_{\imath\in I}A_\imath)^c = \bigcup_{\imath\in I}A_\imath^c.$$

Suppose that A is a non-empty countable set. We have seen that we may write $A = \{a_1, a_2, a_3, \ldots\}$. When A is indexed by $\imath$ we write

$$A = A_\imath = \{a_{\imath,1},\, a_{\imath,2},\, a_{\imath,3},\, \ldots\} \tag{3}$$

where $a_{\imath,n} = a_n$ for all $n \geq 1$. The following proposition generalizes Corollary 2.

Proposition 2 *Let $\{A_\imath\}_{\imath\in I}$ be a family of countable sets indexed by a non-empty countable set I and suppose that at least of the the $A_\imath$'s is denumerable. Then $\bigcup_{\imath\in I}A_\imath$ is denumerable.*

Proof: We may assume that $A_\ell \neq \emptyset$ for all $\ell \in I$. For by assumption $A_\jmath$ is denumerable for some $\jmath \in I$. Therefore there is an $a \in A_\jmath$. If $A_\ell = \emptyset$ replace A_ℓ by $A_\ell = \{a\}$. This does not change the union.

Write $A_\imath$ as in (3) for all $\imath \in I$. The map $f : I\times\mathbf{Z}^+ \longrightarrow \bigcup_{\imath\in I}A_\imath$ defined by $f((\imath, n)) = a_{\imath,n}$ is a surjection. Now $I\times\mathbf{Z}^+$ is denumerable by Corollary 3. By assumption one of the $A_\imath$'s, say $A_\jmath$, is denumerable. Since $A_\jmath \subseteq \bigcup_{\imath\in I}A_\imath$ it follows that $\bigcup_{\imath\in I}A_\imath$ is infinite. Therefore $\bigcup_{\imath\in I}A_\imath$ is denumerable by Proposition 1. □

We apply the preceding proposition to show that the set of real algebraic numbers is denumerable. A real number r is said to be *algebraic* if for some $n \geq 1$ there are rational numbers $a_0, a_1, \ldots, a_n$, not all of which are zero, such that

$$a_0 + a_1r + \cdots + a_nr^n = 0. \tag{4}$$

Let $f = f(x) = a_0+a_1x+\cdots+a_nx^n$ be the polynomial function with rational coefficients suggested by (4). Then $f(r) = 0$. Thus the real algebraic numbers are simply the zeros of the non-zero polynomial functions with rational coefficients. By the results of Calculus $f(x)$ has at most n-zeros. Thus

$$V_f = \{x \in \mathbf{R} \,|\, f(x) = 0\} \qquad \text{is finite,}$$

since $f \neq 0$, and all real algebraic numbers belong to such a V_f.

For the zero polynomial we set $V_0 = \mathbf{Q}$. Note that every rational number a is a real algebraic number since a is a zero of the non-zero polynomial function $x - a$ with rational coefficients. Let $\mathcal{P}$ be the set of polynomial functions with rational coefficients. Then the set of real algebraic numbers is

$$\bigcup\nolimits_{f\in\mathcal{P}} V_f,$$

which the the union of countable sets, one of which (namely V_0) if denumerable. Once we show that $\mathcal{P}$ is countable we can conclude that the preceding union is denumerable by Proposition 2.

For $n \geq 1$ let

$$\mathcal{P}_n = \{f(x) \,|\, f(x) = a_0 + a_1x + \cdots + a_nx^n \ \text{ for some } a_0, a_1, \ldots, a_n \in \mathbf{Q}\}.$$

Then $\mathcal{P} = \bigcup_{n=1}^{\infty}\mathcal{P}_n$. Since each $\mathcal{P}_n$ contains the linear functions $x - a$, where $a \in \mathbf{Q}$, it follows that $\mathcal{P}_n$ is infinite for all $n \geq 1$.

For all $n \geq 1$ note that the function

$$\mathbf{Q}\times\cdots\times\mathbf{Q} \longrightarrow \mathcal{P}_n$$

given by

$$(a_0, a_1, \ldots, a_n) \mapsto f(x) = a_0 + a_1x + \cdots + a_nx^n$$

is a surjection. Since $\mathbf{Q}$ is denumerable by Corollary 4, the Cartesian product is denumerable by Corollary 3. Thus $\mathcal{P}_n$ is denumerable by Proposition 1. Therefore $\mathcal{P} = \bigcup_{n=1}^{\infty}\mathcal{P}_n$ is denumerable by Proposition 2. We have shown that $\mathcal{P}$ is countable.