

## Math 310 Class Notes 6: Countability

Let us first solve the midterm problem 4 before we bring up the related issues.

**Theorem 1.** *Let  $I_n := \{k \in \mathbb{N} : k \leq n\}$ . Let  $f : I_n \rightarrow \mathbb{N}$  be a one-to-one function and let  $Im(f)$  be the image (range) of  $f$  in  $\mathbb{N}$ . Then there is a one-to-one function  $g : I_n \rightarrow Im(f)$  such that  $g$  is order-preserving in the sense that  $g(x) < g(y)$  if  $x < y$ .*

*Proof.* Let us do induction on  $n$ . For  $n = 1$ , there is nothing to prove. Suppose the statement is true for  $n$ . Let  $f : I_{n'} \rightarrow \mathbb{N}$  be one-to-one. Let  $l \in I_{n'}$  be such that  $w := f(l)$  is the least element of  $Im(f)$  whose existence is guaranteed by the well-ordering principle.

Define a function  $h : I_n \rightarrow Im(f) \setminus \{w\}$  given by  $h(z) = f(z)$  for  $z < l$  and  $h(z) = f(z+1)$  for  $z \geq l$ . Then  $h$  is one-to-one and onto (why?), so that by the induction hypothesis there is an order-preserving function  $k : I_n \rightarrow Im(f) \setminus \{w\}$ . Now define the function  $g : I_{n'} \rightarrow Im(f)$  such that  $g(1) = w$  and  $g(z) = k(z-1)$  for  $z \geq 2$ . It is readily checked that  $g$  is one-to-one and onto and order-preserving (why?).  $\square$

**Corollary 2.** *If  $f : I_m \rightarrow I_n$  is one-to-one, then  $m \leq n$ . In particular, if  $f$  is one-to-one and onto, then  $m = n$ .*

*Proof.* By Theorem 1, there is a one-to-one and onto function  $g : I_m \rightarrow Im(f)$  such that  $g$  is order-preserving. We claim that  $g(x) \geq x$  for all  $x \in I_m$ . Suppose this is not the case. Then there is a least element  $k$  in  $I_m$  such that  $g(k) < k$ . It is clear that  $k > 1$  as  $g(1) \geq 1$  always holds. Now  $g(k-1) \geq k-1$ , and so by the fact that  $g$  is order-preserving we have

$$g(k) > g(k-1) \geq k-1,$$

so that  $g(k) \geq k$ . This is a contradiction. Thus  $g(x) \geq x$  for all  $x \in I_m$ . But then as  $g(m) \in I_n$  we see

$$n \geq g(m) \geq m.$$

This settles the first statement.

When  $f$  is one-to-one and onto,  $f^{-1}$ , the inverse function to  $f$ , is also one-to-one. Hence we also have  $n \leq m$  for  $f^{-1}$  in addition to  $m \leq n$  for  $f$ . So  $m = n$ .  $\square$

**Definition 3.** *A set  $S$  is said to be a finite set if there is a bijective (one-to-one and onto) function  $f : I_m \rightarrow S$  for some  $m \in \mathbb{N}$ .  $m$  is called the cardinality of  $S$ . Otherwise,  $S$  is said to be an infinite set.*

Note that the cardinality of a finite set is well-defined. This is because if  $f : I_n \rightarrow S$  and  $g : I_m \rightarrow S$  are both bijective, then  $g^{-1} \circ f : I_n \rightarrow I_m$  is bijective, so that  $m = n$  by Corollary 2.

**Theorem 4.** *Any subset of  $I_m$  is a finite set. More generally, any subset of a finite set is a finite set; in particular, if  $A$  is an infinite subset of  $B$ , then  $B$  is infinite.*

*Proof.* It suffices to prove the first statement, for which we use induction on  $n$ . The statement is automatically true for  $n = 1$ . Suppose it is true for  $n$ . Let  $S$  be a subset of  $I_{n'}$ . If  $S \subset I_n$ , then the induction hypothesis implies that  $S$  is a finite set; the induction is complete. Otherwise  $n' \in S$ . The set  $S_1 = S \setminus \{n'\}$  is a subset of  $I_n$ , so that by the induction hypothesis there is a bijective function  $f : I_m \rightarrow S_1$ , with  $m \leq n$  by Corollary 2. The function  $g : I_{m'} \rightarrow S$  defined by  $g(z) = f(z)$  for  $z \in I_m$  and  $g(m') = n'$  is bijective, proving that  $S$  is a finite set. The induction is done.  $\square$

**Definition 5.** *A set  $S$  is said to be countable if there is a bijective function  $f : \mathbb{N} \rightarrow S$ .*

**Theorem 6.**  *$\mathbb{N}$  is an infinite set.*

*Proof.* Suppose  $\mathbb{N}$  is finite. Let  $f : I_m \rightarrow \mathbb{N}$  be a bijective function for some  $m \in \mathbb{N}$ . By Theorem 1 we know there is a bijective function  $g : I_m \rightarrow Im(f)$  that is also order-preserving. But then all the elements of  $Im(f)$  will be no greater than  $g(m)$ , and since  $Im(f) = \mathbb{N}$  by the assumption that  $f$  is an onto map, we are forced to have that all natural numbers will be no greater than  $g(m)$ . This is absurd as  $g(m) + 1 > g(m)$ . Hence  $\mathbb{N}$  is infinite.  $\square$

**Corollary 7.** *Any countable set is an infinite set.*

*Proof.* Otherwise, there would be a bijective function  $f : I_m \rightarrow S$  for some  $m \in \mathbb{N}$ . However, there is a bijective function  $g : \mathbb{N} \rightarrow S$ . Hence, the bijective composite function  $g^{-1} \circ f : I_m \rightarrow \mathbb{N}$ , where  $g^{-1}$  denotes the function inverse to  $g$ , would make  $\mathbb{N}$  a finite set, which is absurd.  $\square$

Before proving the next theorem, let us look at a generalized recursion theorem.

**Theorem 8.** *Let  $V$  be a set and let  $f : V \rightarrow V$  be a function. Let  $c$  be a fixed element in  $V$ . Then there is a unique function  $g : \mathbb{N} \rightarrow V$  such that  $g(1) = c$  and  $g(x') = f(g(x))$ .*

*Proof.* It goes verbatim with the proof of the recursion theorem in Class Notes 5. The only change is that we must consider the set  $\mathbb{N} \times V$  when coming up with the function  $g$ , as its range lies in  $V$ .  $\square$

**Theorem 9.** *Let  $S$  be an infinite subset of  $\mathbb{N}$ . Then  $S$  is countable.*

*Proof.* Let  $V$  be the power set of  $\mathbb{N}$ ; the elements of  $V$  are all subsets of  $\mathbb{N}$ . Consider the function  $f : V \rightarrow V$  defined by

$$f : A \subset \mathbb{N} \mapsto A \setminus \{\text{the least element of } A\}$$

if  $A \neq \emptyset$ , and defined by  $f(\emptyset) = \emptyset$ .

Let  $c = S$  in  $V$ . Then by Theorem 8, there is a function  $g : \mathbb{N} \rightarrow V$  such that  $g(1) = S$  and  $g(x') = f(g(x))$ . To illustrate,  $g(1) = S, g(2) = S \setminus \{\text{the least element of } S\} := S_1, g(3) = S_1 \setminus \{\text{the least element of } S_1\} := S_2$ , etc.

We first claim that when  $x < y$ , then the least element of  $g(x)$  does not belong to  $g(y)$ , so long as  $g(x) \neq \emptyset$ . We fix  $x$  and do induction on  $k \in \mathbb{N}$  with  $y = x + k$ . For  $k = 1$  we have  $y = x'$ . Since  $g(x') = g(x) \setminus \{\text{the least element of } g(x)\}$ , the statement is certainly true. Assume the statement is true for  $k$  with  $y = x + k$ . That is, we have now  $x < y$  and the least element of  $g(x)$  does not belong to  $g(y)$ . Then  $g(y') = g(y) \setminus \{\text{the least element of } g(y)\}$  and so certainly the least element of  $g(x)$  does not belong to  $g(y')$  with  $y' = x + k'$ . So the statement holds for  $k'$ . The induction is completed and the claim proven.

We claim next that  $g(x) \neq \emptyset$  for all  $x \in \mathbb{N}$ .

Suppose the contrary. Then there is an  $x \in \mathbb{N}$  for which  $g(x) = \emptyset$ . By the well-ordering principle, there is a least  $m \in \mathbb{N}$  such that  $g(m) = \emptyset$ . Note that  $m > 1$  as  $g(1) = S \neq \emptyset$  since  $S$  is infinite. It follows that for all natural numbers  $k < m$ , we have  $g(k) \neq \emptyset$ .

Consider the function  $H : I_{m-1} \rightarrow S \subset \mathbb{N}$  defined by

$$H : k \mapsto \text{the least element of } g(k)$$

for  $1 \leq k \leq m - 1$ .

We show  $H$  is one-to-one. This is because we have verified four paragraphs above that if  $1 \leq k < l \leq m - 1$  then the least element of  $g(k)$  does not belong to  $g(l)$ , whereas  $H(k) = H(l)$  would force the least element of  $g(k)$  to belong to  $g(l)$ , which is impossible.

We show  $H$  is onto. Suppose the contrary. Then there is an element  $z \in S$  such that  $z$  is not the least element of any  $g(k), 1 \leq k \leq m - 1$ . We claim that  $z \in g(y)$  for all  $1 \leq y \leq m - 1$ . This is true for  $y = 1$  because  $g(1) = S$  and  $z \in S$ . Suppose the claim is not true; let  $k, 2 \leq k \leq m - 1$ , be the least natural number such that  $z \notin g(k)$ . Since now  $z \in g(k - 1)$ , the fact that  $g(k) = g(k - 1) \setminus \{\text{the least element of } g(k - 1)\}$

1) $\}$ ,  $z \in g(k-1)$  and  $z$  is not the least element of  $g(k-1)$  imply that  $z \in g(k)$ . This is a contradiction. Therefore,  $z \in g(y)$  for all  $1 \leq y \leq m-1$ ; in particular  $z \in g(m-1)$ . But then, exactly the same argument establishes that  $z \in g(m) = \emptyset$ , which is absurd. So,  $H$  is onto.

That  $H$  is one-to-one and onto means that  $S$  is a finite set, which contradicts the infinitude of  $S$ . The contradiction verifies the validity of the claim that  $g(x) \neq \emptyset$  for all  $x \in \mathbb{N}$ .

Define now the function  $K : \mathbb{N} \rightarrow S$  given by

$$K : x \mapsto \text{the least element of } g(x).$$

An easy induction argument warrants that  $K$  is order-preserving, that is,  $K(x) < K(y)$  if  $x < y$  (why?). It follows from another easy induction argument that  $K(x) \geq x$  for all  $x \in \mathbb{N}$  (why?).

The same argument for the function  $H$  ensures that  $K$  is one-to-one.

We show  $K$  is onto. Suppose  $K$  is not onto; let  $z \in S \setminus \text{Im}(K)$ . Then an induction argument similar to that for  $H$  gives that  $z \in g(x)$  for all  $x \in \mathbb{N}$ , which forces that

$$z > \text{the least element of } g(x) = K(x) \geq x$$

for all  $x \in \mathbb{N}$ . This is absurd. Hence  $K$  is onto.

In conclusion,  $S$  is countable. □

**Corollary 10.** *Let  $f : \mathbb{N} \rightarrow S$  be an onto function. If  $S$  is an infinite set, then  $S$  is a countable set.*

*Proof.* Since  $f$  is an onto map, we know for each  $y \in S$ , there is an  $x \in \mathbb{N}$  such that  $f(x) = y$ . Let  $T_y$  be the subset of  $\mathbb{N}$  consisting of natural numbers  $m$  such that  $f(m) = y$ . Then  $T_y$  is not empty as  $x$  is in it. Hence the well-ordering principle implies that  $T_y$  has the least element; call it  $n_y$ .

Consider the function  $h : S \rightarrow \mathbb{N}$ , where  $h(y) = n_y$ . (Why is  $h$  a function?) Observe  $h$  is one-to-one (why?) so that it follows that  $\text{Im}(h)$  is an infinite subset of  $\mathbb{N}$  (why?). Therefore,  $\text{Im}(h)$  is countable by Theorem 9. Hence  $S$  is also countable (why?). □

**Corollary 11.** *Let  $S$  be a countable set and let  $f : S \rightarrow T$  be an onto function. If  $T$  is infinite, then  $T$  is countable.*

*Proof.* Why? □

**Corollary 12.** *Let  $A$  and  $B$  be two countable sets. Then  $A \cup B$  is countable.*

*Proof.* Let  $f : \mathbb{N} \rightarrow A$  and  $g : \mathbb{N} \rightarrow B$  be two one-to-one and onto functions identifying  $\mathbb{N}$  with  $A$  and  $B$ , respectively. Consider the set

$$C := \{(n, z_n) : n \in \mathbb{N}, z_n \in A \cup B, z_n = f(k) \text{ if } n = 2k, \text{ and } z_n = g(k) \text{ if } n = 2k+1\}$$

$C$  is countable via the function  $n \mapsto (n, z_n)$ . Now consider the onto map  $\pi : C \rightarrow A \cup B$  defined by

$$\pi : (n, z_n) \mapsto z_n.$$

Since  $A$  is countable and hence infinite by Corollary 7, we see  $A \cup B$  is also infinite by Theorem 4. Then the ontoness of  $\pi$  and Corollary 11 applied to  $\pi$  assert that  $A \cup B$  is countable.  $\square$

**Theorem 13.**  $\mathbb{N} \times \mathbb{N}$  is countable. More generally, if  $A$  and  $B$  are countable sets, then  $A \times B$  is countable.

*Proof.* For any  $(p, q) \in \mathbb{N} \times \mathbb{N}$  with  $p + q = n + 1$  we define the function  $F : (p, q) \in \mathbb{N} \times \mathbb{N} \mapsto q + (n - 1)n/2 \in \mathbb{N}$ . Check  $F$  is one-to-one and onto. (Why is this true?)  $\square$

**Corollary 14.**  $\mathbb{Q}$  is countable.

*Proof.* By Corollary 12, it suffices to show that  $\mathbb{Q}^+$ , the set of positive rational numbers is countable. Consider the map  $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Q}^+$  given by

$$f : (m, n) \mapsto n/m.$$

Now  $\mathbb{Q}$  is an infinite set as it contains  $\mathbb{N}$ . Corollary 11 and Theorem 13 then finish the proof.  $\square$

**Definition 15.** A set  $S$  is said to be uncountable if it is neither finite nor countable.

**Theorem 16.** The power set  $2^{\mathbb{N}}$  of  $\mathbb{N}$  is uncountable.

*Proof.*  $2^{\mathbb{N}}$  is the set whose elements are all subsets of  $\mathbb{N}$ .

Suppose  $2^{\mathbb{N}}$  is countable and let  $f : \mathbb{N} \rightarrow 2^{\mathbb{N}}$  be a one-to-one and onto function. Consider the set

$$S := \{x \in \mathbb{N} : x \notin f(x)\}.$$

Since  $S \in 2^{\mathbb{N}}$  and since  $f$  is onto, we see there is a  $y \in \mathbb{N}$  such that  $f(y) = S$ .

If  $y \in f(y) = S$ , then  $y \notin f(y)$  by the definition of  $S$ ; this is a contradiction. So,  $y \notin f(y)$ . But then  $y \in S = f(y)$  by the definition of  $S$ . This is again a contradiction. Therefore,  $f$  does not exist. That is,  $2^{\mathbb{N}}$  is uncountable.  $\square$

**Remark 17.** *More generally, the method in Theorem 16 shows that there are no onto functions from any set  $A$  to its power set  $2^A$ , though there is a one-to-one function from  $A$  to  $2^A$  that sends  $a \in A$  to  $\{a\} \in 2^A$ .*

**Definition 18.** *We say set  $A$  and set  $B$  have the same cardinality, denoted  $\text{card}(A) = \text{card}(B)$ , if there is a one-to-one and onto function between them.*

**Theorem 19.**  $\text{card}(\mathbb{R}) = \text{card}(2^{\mathbb{N}})$ .

The proof will be given in class.

**Definition 20.** *We say set  $A$  is dominated by set  $B$ , denoted  $\text{card}(A) \leq \text{card}(B)$ , if there is a one-to-one function  $f : A \rightarrow B$ .*

*We say set  $A$  is strictly dominated by set  $B$ , denoted  $\text{card}(A) < \text{card}(B)$ , if  $A$  is dominated by  $B$  and there are no functions  $g$  that map  $A$  one-to-one and onto  $B$ .*

Intuitively,  $A$  is strictly dominated by  $B$  if the size of  $A$  is smaller than the size of  $B$ .

A set is thus strictly dominated by its power set by Remark 17. In particular,  $\text{card}(\mathbb{N}) < \text{card}(\mathbb{R})$  by Theorem 19.

**Cantor's Continuum Hypothesis.** There are no sets  $A$  satisfying  $\text{card}(\mathbb{N}) < \text{card}(A) < \text{card}(\mathbb{R})$ .

Through Kurt Gödel and Paul Cohen's deep works, we know the Continuum Hypothesis is independent of the axioms of set theory!

### A Final Remark About The Axiom Of Choice

We know  $\mathbb{N}$  is well-ordered with respect to the standard  $<$  we have defined. The question naturally arises as to whether every set can be well-ordered.

**Definition 21.** *A relation  $<$  on a set  $S$  is said to be an order if for any elements  $x, y \in S$ , one and only one of the following holds: (1)  $x = y$ ; (2)  $x < y$ ; (3)  $y < x$ .*

*A set  $S$  with an order  $<$  is said to be well-ordered by  $<$  if every nonempty subset of  $S$  has the least element.*

For a well-ordered set we have the following induction theorem

**Theorem 22.** *(Transfinite induction) Let  $X$  be well-ordered by  $<$ . Suppose a subset  $S$  of  $X$  has the property:*

$$(*) \quad x \in S \text{ if } \{y \in X : y < x\} \subset S.$$

*Then we conclude  $S = X$ .*

*Proof.* Suppose  $S \neq X$ . Let  $x_0$  be the smallest element of  $X \setminus S$ . Then every  $y < x_0$  lies in  $S$ , since  $x_0$  is the smallest element not in  $S$ . So by (\*) we assert  $x_0 \in S$ , a contradiction. Hence  $S = X$ .  $\square$

Note that if  $y \in X$  is the least element, then  $y \in S$  automatically. This is because the set  $\{z \in X : z < y\} = \emptyset \subset S$ . Therefore,  $y \in S$  by (\*).

Of course, when  $X = \mathbb{N}$  with the usual  $<$ , the transfinite induction is just the mathematical induction.

**Theorem 23.** (*The Well-ordering Principle*) *Every set can be well-ordered if and only if the axiom of choice holds.*

For a proof of this theorem, see *Naive Set Theory* by Paul Halmos. The idea is to utilize the concept of "ordinal" numbers. Therefore, every set can be well-ordered.