

## 6. Cardinality

Roughly, this word means “size.” This lecture deals with the notion of the size of a set. We can use it as a device to catalog sets. In practice, it is also an essential notion in counting problems, some of which we shall study.

### 6.1. Size by comparison

We can say that the set  $\{Curly, Larry, Moe\}$  has exactly 3 members because we can associate its members to the counting numbers 1,2,3 in a one-to-one fashion. More generally, for  $n \in \mathbf{N}$ , we say that a set  $A$  has a *cardinality*  $n$  if there is a bijection

$$f : \{1, 2, \dots, n\} \rightarrow A.$$

In this case, we also say that  $A$  is *finite*. By definition, the empty set is finite with cardinality 0. A bijection can be thought of as associating members of  $A$  to the counting numbers 1,2,..., $n$  in a one-to-one fashion without leaving out or double counting any members of  $A$ .

Why can't a finite set have two different cardinalities? For example, the identity function

$$f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}, \quad f(k) = k$$

is a bijection, which implies that  $\{1, 2, \dots, n\}$  itself has a cardinality  $n$ . Why can't this set have a different cardinality?

We say that a set  $A$  is *infinite* if it is not finite, i.e. if there it is nonempty and if there is no bijection  $f : \{1, 2, \dots, n\} \rightarrow A$ , for any  $n \in \mathbf{N}$ . How do we “measure” the size of

an infinite set? The idea is to use certain well-known infinite sets as “standards” for sizes, in much the same way we use sets like  $\{1, 2, \dots, n\}$  to measure the sizes of finite sets. For example,  $\mathbf{N}$ ,  $\mathbf{Z}$ ,  $\mathbf{Q}$ ,  $\mathbf{R}$  are infinite sets we know relatively well. Given a set  $A$ , we say that it has a *countable* cardinality or that it is countable, if there is a bijection

$$f : \mathbf{N} \rightarrow A.$$

We say that an infinite set is *uncountable* if it is not countable, i.e. there is no bijection from  $\mathbf{N}$  to the set.

We have introduced three important attributes for sets: *finiteness*, *countability* and *cardinality*. In this lecture, we will see that the cardinality of a finite set is unique. We will also see that  $\mathbf{N}$ ,  $\mathbf{Z}$  and  $\mathbf{Q}$  are countable sets, and that  $\mathbf{R}$  is uncountable. These examples motivate the following.

**Definition 6.1.** *Let  $A$  and  $B$  be sets. We say that  $B$  has larger cardinality than  $A$ , if there is an injection but no bijection from  $A$  to  $B$ .*

Thus, as we shall see,  $\mathbf{R}$  has larger cardinality than  $\mathbf{N}$ . It is important to note that even though there are more members in  $\mathbf{Z}$  than  $\mathbf{N}$ ,  $\mathbf{Z}$  does not have larger cardinality than  $\mathbf{N}$ . Thus comparing cardinalities of two sets is more than comparing their memberships. It is about comparing the sets using functions from one set to another.

*Given a set  $A$ , is there always a set which has larger cardinality than  $A$ ?* This question together with all three set attributes introduced above are based on the notion of bijections or more generally, functions. So, we now return to this topic and develop further concepts and properties about functions to study the three attributes for sets. We will then return to the questions raised in this introduction.

## 6.2. Functions revisited

*The identity function.* For any given set  $A$ , the function

$$id_A : A \rightarrow A, \quad id_A(x) = x$$

is called the identity function on  $A$ .

*Composition.* Let  $A, B, C$  be sets,  $f : A \rightarrow B$  and  $g : B \rightarrow C$  be functions. We define a third function

$$g \circ f : A \rightarrow C, \quad (g \circ f)(x) = g(f(x)).$$

This function is called the composition of  $g$  with  $f$ . It is important to keep in mind that it does not make sense to compose two functions unless the domain of one function is the target of the other, as in the preceding definition.

**Exercise.** Given  $f : A \rightarrow B$ , verify that

$$f \circ id_A = id_B \circ f = f.$$

**Proposition 6.2.** (*Associativity of Composition*) Let  $A, B, C, D$  be sets,  $f : A \rightarrow B$ ,  $g : B \rightarrow C$ , and  $h : C \rightarrow D$  be functions. Then

$$(g \circ f) \circ h = g \circ (f \circ h).$$

Proof: To say that two functions are equal is to say that they have the same domain, the same target, and the same value at each point  $x$  of the domain. The functions  $h \circ (g \circ f)$  and  $(h \circ g) \circ f$  both have the domain  $A$  and the same target  $D$ . We now verify that they have the same value at each  $x \in A$ :

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))), \quad ((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$$

which are equal.  $\square$

It follows that we can write both  $(g \circ f) \circ h$  and  $g \circ (f \circ h)$  as  $g \circ f \circ h$  without confusion.

**Example.** Recall that if  $f : A \rightarrow B$  is a bijection and  $f^{-1} : B \rightarrow A$  its inverse function, then

$$f^{-1}(f(x)) = x, \quad f(f^{-1}(y)) = y$$

for all  $x \in A$  and  $y \in B$ . It follows that  $f^{-1} \circ f = id_A$  and  $f \circ f^{-1} = id_B$ . The Bijectivity Test can now be restated using the notion of composition.

**Proposition 6.3.** (*Bijection Test*) A function  $f : A \rightarrow B$  is a bijection if and only if there is a function  $g : B \rightarrow A$  such that

$$g \circ f = id_A, \quad f \circ g = id_B.$$

In this case,  $g = f^{-1}$ .

**Corollary 6.4.** If  $f : A \rightarrow B$  and  $g : B \rightarrow C$  are bijections, then  $g \circ f$  is also a bijection whose inverse is  $f^{-1} \circ g^{-1}$ .

Proof: Note that  $g \circ f : A \rightarrow C$  and  $f^{-1} \circ g^{-1} : C \rightarrow A$ . We have

$$g \circ f \circ f^{-1} \circ g^{-1} = g \circ id_B \circ g^{-1} = g \circ g^{-1} = id_C.$$

Likewise  $f^{-1} \circ g^{-1} \circ g \circ f = id_A$ . By the Bijection Test,  $g \circ f$  is a bijection with inverse  $f^{-1} \circ g^{-1}$ .  $\square$

**Exercise.** *Invariance of Injectivity and Surjectivity.* Let  $g : A \rightarrow B$  and  $h : C \rightarrow D$  be bijections, and  $f : B \rightarrow C$  a function. If  $h$  is injective, so is  $h \circ f \circ g$ . If  $h$  is a surjection, so is  $h \circ f \circ g$ . In other words, the properties of injectivity and surjectivity are not affected by composing with a bijection on the left or the right.

### 6.3. Finite sets

For convenience, let us denote the set  $\{1, 2, \dots, n\}$  by  $[n]$ , for  $n \in \mathbf{N}$ .

**Proposition 6.5.** (*Invariance of Finiteness*) Let  $A$  be a finite set that has a cardinality  $n$ . If there is a bijection from  $A$  to a set  $B$ , then  $B$  is finite and has a cardinality  $n$ .

Proof: Let  $f : [n] \rightarrow A$  and  $g : A \rightarrow B$  be bijections. Then  $g \circ f : [n] \rightarrow B$  is a bijection, and so  $n$  is a cardinality of  $B$ . In particular,  $B$  is finite.  $\square$

**Proposition 6.6.** For  $m, n \in \mathbf{N}$ , if there is a bijection  $f : [m] \rightarrow [n]$  then  $m = n$ .

Proof: For  $m \in \mathbf{N}$ , let  $P(m)$  be the statement that if  $n \in \mathbf{N}$  and if  $f : [m] \rightarrow [n]$  is a bijection then  $m = n$ .  $P(1)$  is the statement that if  $n \in \mathbf{N}$  and if  $f : [1] \rightarrow [n]$  is a

bijection then  $1 = n$ , which is true. Take  $m \in \mathbf{N}$ . Assume  $P(m)$ . To prove  $P(m + 1)$ , let  $f : [m + 1] \rightarrow [n]$  be a bijection. Since  $m + 1 \geq 2$ , we have  $n \geq 2$ . We will prove that  $m + 1 = n$ .

Case 1: Suppose  $f(m + 1) = n$ . Then the function  $[m] \rightarrow [n - 1]$ ,  $k \mapsto f(k)$ , is also a bijection. By  $P(m)$ , it follows that  $m = n - 1$ , proving  $P(m + 1)$  in this case.

Case 2: Suppose  $f(m + 1) \neq n$ . The idea is to find a bijection  $g : [n] \rightarrow [n]$  that switches  $n$  with  $f(m + 1)$  and compose it with  $f$  to get a new bijection  $g \circ f : [m + 1] \rightarrow [n]$  that sends  $m + 1$  to  $n$  as in Case 1. So, define

$$g : [n] \rightarrow [n], \quad g(k) = \begin{cases} k & \text{if } k \neq n, f(m + 1) \\ n & \text{if } k = f(m + 1) \\ f(m + 1) & \text{if } k = n. \end{cases}$$

Note that  $g$  is a bijection (in fact,  $g^{-1} = g$ .) Put  $h = g \circ f : [m + 1] \rightarrow [n]$ , which is also a bijection, by the corollary to the Bijectivity Test above. Note that  $h(m + 1) = g(f(m + 1)) = n$ . Thus we can apply the result in Case 1 to the bijection  $h$ , and conclude that  $m + 1 = n$ , proving  $P(m + 1)$  also in this case.  $\square$

**Corollary 6.7.** (*Invariance of Cardinality.*) *Let  $A$  be a finite set that has a cardinality  $m$  and  $B$  a finite set that has a cardinality  $n$ . If there is bijection from  $A$  to  $B$ , then  $m = n$ .*

Proof: Let  $f : A \rightarrow B$ ,  $g : [m] \rightarrow A$  and  $h : [n] \rightarrow B$  be bijections. Then  $h^{-1} \circ f \circ g : [m] \rightarrow [n]$  is a bijection, and so  $m = n$  by the proposition.  $\square$

Specializing this to the case  $A = B$  and the bijection  $id_A : A \rightarrow A$ , we see that *a finite set  $A$  cannot have two different cardinalities.* This answers a question in the beginning of this lecture.

**Example.** *Power set.* For any given set  $A$ , recall that its power set  $P(A)$  is the set consisting of all subsets of  $A$ . We have seen that  $P([n])$  has exactly  $m = 2^n$  members. If  $a_1, \dots, a_m$  is the list of all such members, then the function  $[m] \rightarrow P([n])$ ,  $k \mapsto a_k$  is a bijection. So, the cardinality of  $P([n])$  is  $m = 2^n$ , as expected.

**Exercise.** Show that for  $n \in \mathbf{N}$ , if  $f : A \rightarrow [n]$  is an injection then the cardinality of  $A$  is  $\leq n$ . (Hint: Use induction; in the inductive step, consider  $f : A \rightarrow [n + 1]$  injective but

not surjective. Modify  $f$  if necessary, so that  $n + 1 \notin f(A)$ .) Conclude that any subset of a finite set is finite.

#### 6.4. Representations of natural numbers

**Definition 6.8.** Let  $q$  be a natural number  $> 1$ . A  $q$ -ary number or base  $q$  number is a list  $a_m, \dots, a_0$  of integers, each in  $\{0, 1, \dots, q-1\}$  with  $a_m \neq 0$ . We say that the  $q$ -ary number  $a_m, \dots, a_0$  represents  $n \in \mathbf{N}$ , if  $n = \sum_{i=0}^m a_i q^i$ . The  $a$ 's are called the  $q$ -ary digits of  $n$ , in this case. We usually write a  $q$ -ary number without the commas, and indicate the base  $q$  by using a subscript  $q$ . The terms *binary*, *ternary*, and *decimal* refer to base 2, 3, and 10 respectively. Unless otherwise specified, we usually use decimal numbers to represent natural numbers.

The binary number  $1010_2$  represents the natural number  $2^3 + 2 = 10_{10} = 10$ . The ternary number  $121_3$  represents  $3^2 + 2 \cdot 3^1 + 3^0 = 16$ . The base 3 representations for the first 10 natural numbers are (suppressing subscript 3)

$$1, 2, 10, 11, 12, 20, 21, 22, 100, 101.$$

Note that the coefficient of the highest power of  $q$  always appear on the *left* in a  $q$ -ary number as the leading digit.

**Example.** *Computing  $q$ -ary representations.* Fix  $q > 1$ . Later, we will show that every  $n \in \mathbf{N}$  has a unique  $q$ -ary representation. Assuming this, let's give a procedure for computing the  $q$ -ary representation of a given number  $n \in \mathbf{N}$ . We start by finding the leading nonzero digits  $a_m$ , and then work our way to the last digit  $a_0$ . We determine  $m$  and  $a_m$  by finding the largest power  $q^m$  and largest *positive* coefficient  $a_m \in \{0, 1, \dots, q-1\}$ , such that

$$n - a_m q^m \geq 0.$$

To find the next digit, we find the largest power  $q^{m-1}$  and largest *nonnegative* coefficient  $a_{m-1} \in \{0, 1, \dots, q-1\}$ , such that

$$n - a_m q^m - a_{m-1} q^{m-1} \geq 0.$$

Continuing this way, until we have found the last digit  $a_0$ .

For example, let's compute the base 5 representation of  $n = 354$ . We have  $375 = 3 \cdot 5^3 > 354 > 2 \cdot 5^3 = 250$ . This yields the leading digit and

$$354 - 2 \cdot 5^3 = 104 \geq 0.$$

Then  $5 \cdot 5^2 = 125 > 104 > 4 \cdot 5^2 = 100$ . So,

$$354 - 2 \cdot 5^3 - 4 \cdot 5^2 = 4 \geq 0.$$

Since  $5^1 > 4 > 0 \cdot 5^1$ , we have

$$354 - 2 \cdot 5^3 - 4 \cdot 5^2 - 0 \cdot 5^1 = 4.$$

So the base 5 representation of 354 is  $2404_5$ .

We now address the existence and uniqueness questions. The pattern in first ten ternary numbers above suggests that if we know the ternary representation  $a_m, \dots, a_0$  of  $n \in \mathbf{N}$ , then we can get the ternary representation of  $n + 1$ , by adding  $1_3$  to  $a_m, \dots, a_0$ , and the rule of addition is the same as in the decimal case: when a digit has value 3 or more, we carry 3 to the next higher digit.

For example,  $222_3$  represents  $2 \cdot 3^2 + 2 \cdot 3^1 + 2 \cdot 3^0 = 2 \cdot 13 = 26$ . And 27 is represented by "adding"  $1_3$  to  $222_3$ . This yields  $1000_3$ . Our existence proof will be by induction.

**Theorem 6.9.** *Every natural number has a unique base  $q$  representation.*

Proof: We will prove existence and uniqueness separately.

For  $n \in \mathbf{N}$ , let  $P(n)$  be the statement that  $n$  has a base  $q$  representation with no leading zeros.  $P(1)$  is true, since  $1_q$  represents 1. Take  $n \in \mathbf{N}$  and assume  $P(n)$  is true. Let  $a_m, \dots, a_0$  be the  $q$ -ary representation of  $n$ . From this, we want to get a  $q$ -ary representation  $b_r, \dots, b_0$  of  $n + 1$ , thereby proving  $P(n + 1)$ .

Case 1: Suppose  $a_m = \dots = a_0 = q - 1$ . Our candidate for a  $q$ -ary representation of  $n + 1$  is the list

$$b_{m+1} = 1, \quad b_m = \dots = b_0 = 0.$$

To show that this is correct, we compute

$$\sum_{i=0}^{m+1} b_i q^i = q^{m+1}.$$

By the geometric formula  $\sum_{j=0}^m x^j = \frac{1-x^{m+1}}{1-x}$ , we have

$$n = \sum_{j=0}^m a_j q^j = (q-1) \sum_{i=0}^m q^i = (q-1) \frac{1-q^{m+1}}{1-q} = q^{m+1} - 1.$$

This shows that  $n+1 = \sum_{i=0}^{m+1} b_i q^i$ , and so the list  $b_{m+1}, \dots, b_0$  is a  $q$ -ary representation of  $n+1$ .

Case 2: Suppose not all  $a_i$  are  $q-1$ . Let  $a_t$  be the lowest  $q$ -ary digit of  $n$  with  $a_t < q-1$ . Our candidate for a  $q$ -ary representation of  $n+1$  is the list

$$b_m = a_m, \dots, b_{t+1} = a_{t+1}, b_t = a_t + 1, b_{t-1} = \dots = b_0 = 0.$$

To show that this is correct, we compute

$$\sum_{i=0}^{m+1} b_i q^i = a_m q^m + \dots + a_{t+1} q^{t+1} + (a_t + 1) q^t.$$

We have

$$n = \sum_{j=0}^m a_j q^j = a_m q^m + \dots + a_t q^t + (q-1) \sum_{i=0}^{t-1} q^i = a_m q^m + \dots + a_t q^t + q^t - 1.$$

This shows that  $n+1 = \sum_{i=0}^{m+1} b_i q^i$ , and so the list  $b_m, \dots, b_0$  is a  $q$ -ary representation of  $n+1$ .

We prove uniqueness by the method of descent. Let  $n \in \mathbf{N}$  be the *smallest* integer that has two distinct  $q$ -ary representations  $a_r, \dots, a_0$  and  $b_s, \dots, b_0$ . First we show that  $r = s$ . Since  $a_r \geq 1$  and all other digits are nonnegative, we have  $n = \sum_{i=0}^r a_i q^i \geq q^r$ . Since the digits  $b_j \leq q-1$ , we have  $n = \sum_{j=0}^s b_j q^j \leq (q-1) \sum_{j=0}^s q^j = q^{s+1} - 1$ . So

$$q^{s+1} - 1 \geq q^r.$$

This shows that  $s+1 > r$ . Interchanging the roles of the two  $q$ -ary representations, we find  $r+1 > s$ . So,  $s+1 > r > s-1$ , which implies that  $r = s$ . Now both  $a_r, b_r$  are positive, so we get two distinct  $q$ -ary representations of  $n - q^r$  if we replace  $a_r, b_r$  by  $a_r - 1$  and  $b_r - 1$ . Thus uniqueness fails for  $n - q^r \in \mathbf{N}$ , which is smaller than  $n$ , a contradiction.

□

**Corollary 6.10.** *Let  $N_q$  be the set of all  $q$ -ary numbers. Then the function*

$$f : N_q \rightarrow \mathbf{N}, \quad a_m, \dots, a_0 \mapsto \sum_{i=0}^m a_i q^i$$

is a bijection.

Proof: The existence part of the preceding theorem says that  $f$  is surjective. The uniqueness part of the theorem says that  $f$  is injective.  $\square$

*Arithmetic of q-ary numbers.* As the first ten ternary numbers suggest, the rules of arithmetic for q-ary numbers is quite similar to the rules for decimal numbers. For example, we can do addition digit by digit starting from the *right* most digit, and we “carry” when a digit is  $q$  or more, just as we carry when a given digit is 10 or more in decimal addition. Thus, we have, in base 3:

$$121 + 111 = 1002.$$

This represents the decimal calculation  $16 + 13 = 29$ . Likewise, we also do subtraction digit by digit, and we can “borrow” from the next higher digit. For example, in base 3,

$$121 - 22 = 22.$$

This represents the decimal calculation  $16 - 8 = 8$ . The rules for multiplication and division for q-ary numbers are also similar to those for decimal numbers. For example,

$$121 \times 21 = 11011.$$

This represents the decimal calculation  $16 \times 7 = 112$ .

*Weights Problem.* Suppose you have a balance and  $k$  different *known* weights. How many different weights can you test for? You have 3 options for each of those  $k$  weights: you can put it on either the left pan or the right pan, or omit it. We exclude the case when none of the  $k$  weights are used. So, there are  $3^k - 1$  ways. But the balance is left-right symmetric, so the net number of positive weights we can test for is *at most*  $(3^k - 1)/2$ . Clearly, the optimum situation is when we are able to test for all weights from 1 through  $(3^k - 1)/2$ , leaving no gaps in between. *Can we find  $k$  different weights that does this?*

Let’s experiment in the case  $k = 2$ . We want to be able to test for weights 1,2,3,4 oz. The two weights 1, 3 oz will work. If you experiment with the case  $k = 3$ , you will find that the three weights 1,3,9 oz will work as well. We will see that in general, the set of  $k$  weights  $S_k = \{1, 3, \dots, 3^{k-1}\}$  will allow us to test for all values  $1, 2, \dots, (3^k - 1)/2$ .

Proof: Let  $f(k) = (3^k - 1)/2$ . Our assertion is that for  $1 \leq n \leq f(k)$ , the set  $S_k$  allows us to balance an object of  $n$  oz. To prove this, it suffices to find  $b_0, \dots, b_{k-1} \in \{-1, 0, 1\}$  such that

$$(*) \quad n = \sum_{i=0}^{k-1} b_i 3^i.$$

Note that the value of  $b_i$  being  $-1$  or  $1$  corresponds to putting the weight of  $3^i$  oz on the same or the opposite pan where  $n$  sits. The value of  $b_i$  being  $0$  corresponds to omitting the weight of  $3^i$  oz. Now  $(*)$  can be achieved if and only if

$$(**) \quad \sum_{i=0}^{k-1} (b_i + 1) 3^i = n + f(k).$$

Here we have used the formula  $\sum_{i=0}^{k-1} 3^i = (3^k - 1)/2 = f(k)$ . Since  $n \leq f(k)$ , we have  $n + f(k) \leq 2f(k) = 3^k - 1$ . By the preceding theorem, there is a unique ternary number  $a_{k-1}, \dots, a_0$  such that  $n + f(k) = \sum_{i=0}^{k-1} a_i 3^i$ . So, the  $b_i = a_i - 1 \in \{-1, 0, 1\}$  make  $(**)$  holds. This proves our assertion.  $\square$

## 6.5. Infinite sets

**Proposition 6.11.**  $\mathbf{N}$  is infinite.

Proof: We want to show that there is no bijection from  $[n]$  to  $\mathbf{N}$ , for any  $n \in \mathbf{N}$ . Given  $n \in \mathbf{N}$  and a function  $f : [n] \rightarrow \mathbf{N}$ , its image is  $\{f(1), \dots, f(n)\}$ , which cannot be equal to  $\mathbf{N}$ . For example, we have  $f(1) + \dots + f(n) + 1 > f(k)$ , for each  $k = 1, \dots, n$ , and so  $f(1) + \dots + f(n) + 1 \in \mathbf{N}$  is not in the image of  $f$ . This shows that there is no bijection from  $[n]$  to  $\mathbf{N}$ , for any  $n \in \mathbf{N}$ .  $\square$

**Example.** Let  $A$  be a set. We say that  $A$  is countable if there is a bijection  $f : \mathbf{N} \rightarrow A$ . In this case, every member of  $A$  appears in the infinite list  $f(1), f(2), f(3), \dots$  exactly once. Conversely, if we can make a list  $a_1, a_2, a_3, \dots$  in which every member of  $A$  appears in it *exactly once*, then we the function  $\mathbf{N} \rightarrow A$ ,  $k \mapsto a_k$ , is clearly a bijection. Therefore, to show that a given set  $A$  is countable, one strategy is to find a way to list its members. Keep in mind that to list means to specify the *first*, the second, and every other entries in the list.

For example, consider the set  $\mathbf{Z}$  of integers. There are many ways to directly list its members. One way is

$$0, -1, 1, -2, 2, \dots$$

More precisely, we put

$$f(k) = \begin{cases} (k-1)/2 & \text{for } k \text{ odd} \\ -k/2 & \text{for } k \text{ even.} \end{cases}$$

Then  $f : \mathbf{N} \rightarrow \mathbf{Z}$  is a bijection (verify it!) This shows that  $\mathbf{Z}$  is countable.

**Exercise.** *Invariance of Countability.* Let  $A$  be a countable set. Show that if there is a bijection from  $A$  and to a set  $B$ , then  $B$  is countable.

It is often a lot easier to list all members of a countable set if we allow some members to appear more than once. Here is an example, let's make a list of all members of  $\mathbf{Q}$ . We will represent each member by a fraction  $p/q$  where  $q > 0$ . For any given  $k \in \mathbf{N}$ , the positive fractions  $p/q$  with  $p+q = k+1$  are  $k/1, (k-1)/2, \dots, 1/k$ , which has  $k$  entries. We can join these finite lists together like

$$1/1, 2/1, 1/2, 3/1, 2/2, 1/3, \dots$$

which clearly include all *positive* fractions. We can also list all negative fractions by simply taking the negatives of those positive fractions above. We can combine the two lists into one, by alternating between the two. By including 0, we get a list containing all members of  $\mathbf{Q}$ :

$$0/1, 1/1, -1/1, 2/1, -2/1, 1/2, -1/2, 3/1, -3/1, 2/2, -2/2, 1/3, -1/3, \dots$$

One problem with this list is that some fractions appear more than once (in fact,  $1 = 1/1 = 2/2 = \dots$  appear infinitely many times.) So, by defining  $f(n)$  to be the  $n$ th entry in this list, we have a function  $f : \mathbf{N} \rightarrow A$  that is surjective but not injective. Thus, we cannot yet conclude that  $A$  is countable. The next result resolves this problem.

**Proposition 6.12.** *Any infinite subset of  $\mathbf{N}$  is countable.*

**Proof:** The idea is to list  $A$  in increasing order using the Well-Ordering Property.

Let  $A$  be an infinite subset of  $\mathbf{N}$ . We will define  $f : \mathbf{N} \rightarrow A$  by induction. Let  $f(1)$  be the least member of  $A$ , which exists by the Well-Ordering Property. Take

$n \in \mathbf{N}$ . Assume that  $f(1), \dots, f(n) \in A$  are defined. Let  $f(n+1)$  be the least member of  $A - \{f(1), \dots, f(n)\}$ . Note that this set is nonempty. For its being empty would imply that  $A \subset \{f(1), \dots, f(n)\}$  would be finite. This completes our definition of  $f : \mathbf{N} \rightarrow A$ . It follows by induction that  $f(n+1) > f(n)$ , for all  $n$ . In particular,  $f$  is injective and  $f(\mathbf{N})$  is infinite, by the Invariance of Finiteness.

To show that  $f$  is surjective. We use proof-by-contradiction. Assume that  $f$  is not surjective, which means that  $A - f(\mathbf{N})$  is a nonempty subset of  $\mathbf{N}$ . Let  $m$  be the least member of  $A - f(\mathbf{N})$ . Since  $f(1)$  is the least member of  $A$ ,  $m > f(1)$ . Since  $f(\mathbf{N})$  is infinite, we have  $f(\mathbf{N}) \not\subset [m]$ . Let  $n \in \mathbf{N}$  be the least number such that  $f(n) > m$ . Then  $f(n) > m > f(n-1)$ . But  $f(n)$  is, by the inductive definition, the least member of  $A - \{f(1), \dots, f(n-1)\}$ . Yet, we have found a smaller  $m \in A - \{f(1), \dots, f(n-1)\}$ , a contradiction. This proves that  $f$  is surjective.  $\square$

**Corollary 6.13.** *Let  $A$  be an infinite set. If there is an injection  $f : A \rightarrow \mathbf{N}$  then  $A$  is countable.*

Proof: Since  $f$  is injective, the function  $A \rightarrow f(A)$ ,  $x \mapsto f(x)$ , is injective. This function is surjective, hence bijective, because its image is  $f(A)$ . Since  $A$  is infinite,  $f(A) \subset \mathbf{N}$  is also infinite, by the Invariance of Finiteness. By the preceding proposition,  $f(A)$  is countable. By the Invariance of Countability,  $A$  is countable.  $\square$

**Exercise.** Show that an infinite subset of a countable set is countable.

**Corollary 6.14.** *Let  $A$  be an infinite set. If there is a surjection  $f : \mathbf{N} \rightarrow A$  then  $A$  is countable.*

Proof: Since  $f$  is surjective, for each  $x \in A$ ,  $f^{-1}(\{x\}) \subset \mathbf{N}$  is not empty and so it has a least member  $n_x$ . Note that  $f(n_x) = x$ . Define  $g : A \rightarrow \mathbf{N}$ ,  $g(x) = n_x$ . It is injective: for if  $x, y \in A$  and  $g(x) = g(y)$ , then  $x = f(n_x) = f(g(x)) = f(g(y)) = f(n_y) = y$ . So, we have an injection  $g : A \rightarrow \mathbf{N}$ . So,  $A$  is countable by the preceding corollary.  $\square$

**Corollary 6.15.**  $\mathbf{Q}$  is countable.

Proof: Recall that  $\mathbf{Q}$  is an infinite set, and we can list *all* its members (with repetitions) as above, say  $a_1, a_2, a_3, \dots$ . Define a function  $f : \mathbf{N} \rightarrow \mathbf{Q}$ ,  $n \mapsto a_n$ . Then  $f$  is surjective. By the preceding corollary,  $\mathbf{Q}$  is countable.  $\square$

**Corollary 6.16.**  $\mathbf{N} \times \mathbf{N}$  is countable.

Proof: We can list all members of this infinite set as follows:

$$(1, 1), (1, 2), (2, 1), (1, 3), (2, 2), (3, 1), \dots$$

This defines a surjection (in fact, a bijection)  $f : \mathbf{N} \rightarrow \mathbf{N} \times \mathbf{N}$ . So,  $\mathbf{N} \times \mathbf{N}$  is countable.  $\square$ .

**Corollary 6.17.** If  $A$  and  $B$  are countable sets, then their Cartesian product  $A \times B$  is countable.

Proof: Let  $f : \mathbf{N} \rightarrow A$  and  $g : \mathbf{N} \rightarrow B$  be bijections. Then the function  $\mathbf{N} \times \mathbf{N} \rightarrow A \times B$ ,  $(m, n) \mapsto (f(m), g(n))$ , is a bijection. (Verify this!) By the proposition and the Invariance of Countability,  $A \times B$  is countable.  $\square$

**Exercise.** (Homework 6) Prove that if  $A_1, A_2, A_3, \dots$  is a list of countable sets, then their union  $\cup_{i \in \mathbf{N}} U_i$  is countable. Note that  $x$  is a member of the union if and only if  $x \in U_i$  for some  $i \in \mathbf{N}$ . (Hint: List the members of the union in an infinite array, and use it to define a surjection  $f : \mathbf{N} \rightarrow A$ .)

**Theorem 6.18.**  $\mathbf{R}$  is uncountable.

It is enough to show that  $\mathbf{R}$  has an uncountable subset. For if  $\mathbf{R}$  were to be countable, then every infinite subset of it would be countable. We will argue that the set  $A$  consisting of  $x \in \mathbf{R}$  such that  $0 < x < 1$  is uncountable. We will sketch the main idea, known as Cantor's diagonal argument.

First, note that every  $x \in A$  can be represented (though not uniquely) by a decimal number  $0.a_1a_2a_3 \cdots$  where  $a_1, a_2, a_3, \dots$  are the decimal digits of  $x$ . Suppose  $A$  is countable. Then we can list all members of  $A$  using their decimal representation

$$\begin{array}{l} 0.a_{11}a_{12}a_{13} \cdots \\ 0.a_{21}a_{22}a_{23} \cdots \\ 0.a_{31}a_{32}a_{33} \cdots \\ \dots \quad \dots \end{array}$$

To get a contradiction, it is enough to construct a decimal number not appearing in this list. For  $n \in \mathbf{N}$ , let  $b_n$  be the remainder of  $(a_{nn} + 1)/10$ . Note that  $b_n \in \{0, 1, \dots, 9\}$  is never equal to  $a_{nn}$ . It follows that the number  $0.b_1b_2b_3 \cdots$  can't be on the list above because it differs from the  $n$ th entry of that list by at least the  $n$ th digit.

## 6.6. Sets with ever larger cardinalities

Let  $n \in \mathbf{N}$ . We have seen that  $P([n])$  has cardinality  $2^n > n$ . Thus there is no bijection from  $[n]$  to  $P([n])$ , but there is clearly an injection. For example,  $f : [n] \rightarrow P([n])$ ,  $f(k) = \{k\}$ , defines an injection. Thus  $P([n])$  has *larger cardinality* than  $[n]$ , in the sense defined in the introduction of this lecture. Now let  $A$  be any set. Again,  $f : A \rightarrow P(A)$ ,  $f(x) = \{x\}$ , defines an injection from  $A$  to its power set. The next theorem says that the  $P(A)$  always has larger cardinality than  $A$ .

**Theorem 6.19.** *Let  $A$  be any given set. Then there is no bijection from  $A$  to  $P(A)$ .*

Proof: The main idea is similar to Cantor's diagonal argument.

Suppose that there is a bijection  $A \rightarrow P(A)$ . We shall derive a contradiction. Recall that we have defined a bijection from  $P(A)$  to the set  $C(A)$  of binary functions on  $A$ . Composing the two bijections, we get a bijection  $f : A \rightarrow C(A)$ . Note that for each  $x \in A$ ,  $f(x) : A \rightarrow \{0, 1\}$  is a binary function. We now define a binary function  $g \in C(A)$  as follows. For any  $x \in A$ , put

$$g(x) = \begin{cases} 0 & \text{if } f(x)(x) = 1 \\ 1 & \text{if } f(x)(x) = 0. \end{cases}$$

Note that  $g(x) \neq f(x)(x)$  for any  $x \in A$ . But, since  $f : A \rightarrow C(A)$  is surjective, we have  $g = f(y)$  for some  $y \in A$ . It follows that  $g(y) = f(y)(y)$ , a contradiction.  $\square$

**Corollary 6.20.**  *$P(\mathbf{N})$  is uncountable.*

Proof: This set is clearly infinite. Thus it is either countable or uncountable. Since there is no bijection from  $\mathbf{N}$  to  $P(\mathbf{N})$ ,  $P(\mathbf{N})$  is uncountable.  $\square$

One of the great questions of the twentieth century in logic is this:

*Given a set  $A$ , is there a set  $B$  such that  $B$  has larger cardinality than  $A$  and that  $P(A)$  has larger cardinality than  $B$ ? In other words,  $B$  has cardinality strictly in between those of  $A$  and  $P(A)$ .*

If  $A = [n]$  with  $n \geq 2$ , (or any other finite set with at least 2 members,) the answer is affirmative, since it is easy to find a subset  $B$  of  $P([n])$  whose cardinality is strictly between  $n$  and  $2^n$ . When  $A$  is infinite, the question is much trickier. For  $A = \mathbf{N}$ , we have the following hypothesis in set theory.

**The Continuum Hypothesis:** *There is not a set  $B$  such that  $B$  is larger than  $\mathbf{N}$  and that  $P(\mathbf{N})$  is larger than  $B$ .*

**Definition 6.21.** *We say that two sets have the same cardinality if there is a bijection from one to the other.*

Another way to state the Continuum Hypothesis is that if  $\mathbf{N} \subset B \subset P(\mathbf{N})$  then either  $B$  and  $\mathbf{N}$  have the same cardinality or that  $B$  and  $P(\mathbf{N})$  have the same cardinality.

**Warning:** Suppose we have a proper subset  $A$  of a set  $B$ . The cardinality of  $A$  and  $B$  may or may not be the same. For example, we have seen that any infinite subset of  $\mathbf{N}$  is countable. Thus  $\mathbf{N}$  and any of its infinite subset have the same cardinality. For another example, consider the set  $A$  consisting of all real numbers  $x$  such that  $0 < x < 1$ . Then  $A$  is a proper subset of  $\mathbf{R}$ . Yet, we have the following bijection  $f : A \rightarrow \mathbf{R}$ ,

$$f(x) = \begin{cases} \frac{x - \frac{1}{2}}{x} & \text{if } x \leq \frac{1}{2} \\ \frac{x - \frac{1}{2}}{1 - x} & \text{if } x \geq \frac{1}{2}. \end{cases}$$

Thus  $A$  and  $\mathbf{R}$  have the same cardinality. We also have the subset  $\mathbf{N} \subset \mathbf{R}$ . But we have seen that  $\mathbf{N}$  and  $\mathbf{R}$  do not have the same cardinality.

The point here is that the set inclusion alone  $A \subset B$  does not tell us whether or not  $A$  and  $B$  have the same cardinality. The notion of cardinality is based on the notion of functions, and only that.