Lecture notes on cardinality and infinite sets (Part I)

Some important results about cardinality of finite sets

Here is an obvious fact that is really easy to prove:

Fact 1. If A, B are finite subsets of a universe U such that $A \subseteq B$ then $|A| \leq |B|$.

Proof. This just follows from the definition of $A \subseteq B$:

$$x \in A \to x \in B,$$

which clearly implies that B has at least as many elements as A and so $|A| \leq |B|$. $\square$

There is some notation which I should have introduced in earlier lectures but could not: for a set A,

$$A^n := A \times A \times \ldots \text{ (n times) } \ldots \times A.$$

Basically, A^n is the cartesian product of A with itself, n times. So, for example, if $A = \{0, 1\}$ then

$$A^3 = A \times A \times A = \{(0,0,0), (0,0,1), (0,1,0), \ldots, (1,1,1)\}.$$

Based on earlier discussions,

$$|A^n| = |A|^n.$$

This is because A^n can be thought of as the set of all sequences/tuples of length n where every entry/element of the tuple/sequence is an element of A. There are n spots to fill in, and for each spot we have $|A|$ choices, and all the choices are "independent", i.e. they don't affect each other, and so the total possibilities are $|A|^n$. We will study this in more detail in CS 206.

We will now prove two important results about the cardinality of finite sets which will also help us later in our discussion about infinite sets and their cardinality.

Fact 2. Let A and B be finite sets of a universe U such that there is an injective function $f : A \to B$. Then $|A| \leq |B|$.

Proof. Recall that

$$Range(f) = \{f(a) | \ a \in A\}.$$

Since f is injective, we know that for all a_1, a_2 in A that are distinct (i.e., $a_1 \neq a_2$) it must be the case that $f(a_1) \neq f(a_2)$. This means that each $a \in A$ will be transformed into a distinct element $f(a) \in B$ by f and so the size of $Range(f)$ is exactly equal to the size of A,

$$|Range(f)| = |A|.$$

Also recall that by the very definition of $Range(f)$, we have that

$$Range(f) \subseteq B,$$

and so using Fact 1 we can say that

$$|Range(f)| \leq |B|.$$

Putting together the two inequalities we obtained, we can say that

$$|A| = |Range(f)| \leq |B|$$

$$\Rightarrow |A| \leq |B|.$$

□

We will now prove a similar fact for when there is is a surjective function between two sets A and B:

Fact 3. Let A and B be finite sets of a universe U such that there is a surjective function $f : A \to B$. Then $|A| \geq |B|$.

Proof. Recall that, if a function is surjective then every element $b \in B$ is a possible output of the function f. In other words, for every $b \in B$ there is some $a \in A$ such that $f(a) = b$. Thus, we can say that

$$Range(f) = B,$$

which implies that

$$|Range(f)| = |B|.$$

Let us now consider the definition of the set $Range(f)$;

$$Range(f) = \{f(a) |\ a \in A\}.$$

From the definition, it should be clear that $Range(f)$ can have at most as many elements as there are in A. This is because by the definition of functions each $a \in A$ can contribute exactly one element to $Range(f)$. Thus,

$$|Range(f)| \leq |A|.$$

Combining the two inequalities we obtained, we can conclude that

$$|B| = |Range(f)| \leq |A|$$

$$\Rightarrow |B| \leq |A|.$$

□

Combining the two facts together leads to a very nice way to characterize finite sets that have the same cardinality:

Fact 4. Two non-empty finite sets A and B have the same cardinality, i.e. $|A| = |B|$, if and only if there is a bijection $f : A \to B$.

Proof. Let us assume we will only encounter non-empty sets for the rest of the proof. Let's first prove one part of the statement: $|A| = |B|$ only if there is a bijection between A and B, which is logically equivalent to saying "If $|A| = |B|$ then there is a bijection between A and B".

Let $|A| = |B| = k$ for some integer $k > 0$ (since A and B are non-empty). This means A and B have the same number of elements. Let us number and order the elements of A and B in some arbitrary manner so that

$$A = \{a_1, a_2, \ldots, a_k\},$$

$$B = \{b_1, b_2, \ldots, b_k\}.$$

Then we can define a bijection between A and B simply as f such that for all $1 \leq i \leq k$

$$f(a_i) = b_i.$$

Let us now prove the other direction of the statement, i.e. if there is a bijection between A and B then $|A| = |B|$. Let $f : A \to B$ be the biection. Since f is a bijection, f must be injective, and so using Fact 2 we can conclude that

$$|A| \leq |B|.$$

Also, f must be surjective and so, using Fact 3, we can conclude

$$|A| \geq |B|.$$

Combining the two inequalities we get

$$(|A| \leq |B|) \wedge (|A| \geq |B|) \to |A| = |B|,$$

which completes the proof of the statement. □

This fact lets us prove all sorts of cool stuff and we will see more applications of this fact in CS 206. Here is one such application

Problem 1. Let $A = \{0, 1\}$. Prove that for all $n \geq 1$

$$|A^n| = |\text{pow}(\{1, 2, 3, \ldots, n\})|.$$

Proof. Let $n \geq 1$ be an arbitrary integer. We will prove that A^n and $\text{pow}(\{1, 2, \ldots, n\})$ have the same cardinality by showing that there is a bijection between them.

Let $f : A^n \to \text{pow}(\{1, 2, \ldots, n\})$ be the function that transforms an n-tuple $(x_1, x_2, \ldots, x_n) \in A^n$ into a subset of $\{1, 2, \ldots, n\}$ (and hence an element of $\text{pow}(\{1, 2, \ldots, n\})$) in the following way:

$$f((x_1, x_2, \ldots, x_n)) = \{i \mid 1 \leq i \leq n \text{ and } x_i = 1\},$$

in other words, given the tuple $(x_1, \ldots, x_n)$, we transform it into the subset of $\{1, 2, \ldots, n\}$ that only contains those numbers i from $\{1, 2, \ldots, n\}$ such that the i^{th} element of the tuple, i.e. x_i, is equal to 1 (recall that every element of the sequence is either 1 or 0), i.e.

$$i \in f((x_1, x_2, \ldots, x_n)) \leftrightarrow x_i = 1.$$

Let us now show that f is a bijection. First, note that f is injective. To see this, consider two distinct elements of A^n, say $(x_1, \ldots, x_n)$ and $(x'_1, \ldots, x'_n)$. Since the two tuples are distinct, they must differ at some position j (otherwise, if they matched at each of the n positions, they would just be equal), i.e. $x_j \neq x'_j$. We can assume that $x_j = 1$ and $x'_j = 0$ (the other case is symmetric). This would mean that

$$j \in f((x_1, \ldots, x_n))$$

but

$$j \notin f((x'_1, \ldots, x'_n)).$$

So

$$f((x_1, \dots, x_n)) \neq f((x'_1, \dots, x'_n)),$$

and f is injective.

Next, we will show f is surjective. Consider an arbitrary subset $S \subseteq \{1, \dots, n\}$. We want to show that there is some tuple $(x_1, \dots, x_n)$ such that

$$f((x_1, \dots, x_n)) = S.$$

This is quite straightforward. Let $(x_1, \dots, x_n)$ be the tuple such that for all $1 \leq i \leq n$

$$x_i = \begin{cases} 1 & \text{if } i \in S \\ 0 & \text{if } i \notin S \end{cases}$$

It easy to convince yourself that because of the way we defined $(x_1, \dots, x_n)$ and the function f, it must be the case that

$$f((x_1, \dots, x_n)) = S.$$

So f is also surjective, and we can finally conclude that f is a bijection. Since f is a bijection between A^n and $\text{pow}(\{1, \dots, n\})$, we can conclude using Fact 4 that

$$|\text{pow}(\{1, \dots, n\})| = |A^n|$$

$\square$

Recall that $|A^n| = |A|^n$, and so from the theorem we just proved we can conclude that

$$|\text{pow}(\{1, \dots, n\})| = |A^n| = |A|^n = |\{0, 1\}|^n = 2^n,$$

i.e., the number of subsets of the set $\{1, \dots, n\}$ is equal to 2^n, a fact we had discussed earlier.

Infinite sets vs finite sets

Most facts and operations we learnt about finite sets work the same way for infinite sets. Operations such as union, intersection, difference, complement, symmetric difference, (See your textbook if you can't remember what these operations are) and rules such as associativity, distributivity, De Morgan's law, etc. (Again, see the textbook if you can't remember what these rules mean), all work the same way as in the case of finite sets.

Even functions defined on infinite sets have the same operations as those defined on finite sets: composition, addition, multiplication, etc., and you can define surjectivity, injectivity, and bijectivity in the same way as you would define for functions on finite sets.

All in all, there isn't any difference between how we study finite and infinite sets, except for one thing: cardinality! Obviously, infinite sets are *not* finite, and are *infinite*. But are all infinite sets of the same? For example, do we think that natural numbers and real numbers are of the same "size"? We will discuss this in detail now.

The cardinality of infinite sets

For finite sets, it is easy to define what cardinality means; it's very natural: it's just the number of elements in the set. We can always imagine finite sets as containers/boxes that contain a bunch of objects inside them.
However, for infinite sets, what does cardinality even mean? How do you define size? Instead of trying to do that, let's try to first come up with a way to define what it means for two infinite sets to be of the same "cardinality"/"size".

Definition 1. Two infinite sets A, B are said to have the same cardinality if there is a bijection between them, i.e. there is a function $f : A \to B$ that is a bijection. We use the notation $|A| = |B|$ to denote that A and B have the same cardinality.

If you think about it a bit, this definition does make sense: a bijection between two sets A and B is a way of pairing elements of A and B, i.e. each element of A gets paired with a unique element of B and vice-versa. Think of the following thought experiment. Suppose there are infinitely many boys and girls in a ballroom and someone tells you that it is possible to pair off each boy with a girl and each girl with a boy to form dancing pairs so that no two people share a partner, wouldn't you be convinced that the number of boys and girls is in some sense the same (again, we are talking about "number of boys and girls" in an intuitive informal way here since the "number" is infinite)? If they were not, how would you even be able to pull off the pairing process?

Definition 2. An infinite set S is said to be *countably infinite* if there is a bijection between S and $\mathbb{N}$.

In the above definition, it is important to keep in mind that when we say "there is a bijection between S and $\mathbb{N}$", we mean either a bijection from S to $\mathbb{N}$ or the other way round, since both are equivalent, i.e. there is an bijection from $\mathbb{N}$ to S if and only if there is a bijection from S to $\mathbb{N}$ (Think of starting with a bijection in one direction and then taking its inverse to get the bijection in the other direction).

Definition 3. A set that is countably infinite is said to have cardinality equal to $\aleph_0$ (pronounced as "aa-lef naught" or "aa-lef zero"), denoted by

$$|S| = \aleph_0.$$

In particular,

$$|\mathbb{N}| = \aleph_0.$$

Is the cardinality of $\mathbb{Z}$ same as of that of $\mathbb{N}$? Surprisingly, the answer is yes!

Problem 2. Show that $\mathbb{Z}$ is countably infinite, i.e.

$$|\mathbb{Z}| = \aleph_0.$$

Proof. We will prove the statement by showing that there is a bijection $f : \mathbb{N} \to \mathbb{Z}$. Consider the following function $f : \mathbb{N} \to \mathbb{Z}$:

$$f(x) = \begin{cases} \frac{x+1}{2} & \text{if } x \text{ is odd} \\ -\frac{x}{2} & \text{if } x \text{ is even.} \end{cases}$$

Let us first prove that f is injective. Let $x_1 \neq x_2$ be two distinct natural numbers.
Case I: (x_1 is odd and x_2 is even, or x_2 is odd and x_1 is even) Note that if x_1 is odd and x_2 is even, then

$$f(x_1) > 0$$
$$f(x_2) < 0$$

by the definition of f, and so $f(x_1) \neq f(x_2)$. The other sub-case also follows from the same proof.
Case II: (x_1, x_2 are both odd): In this case,

$$f(x_1) = \frac{x_1 + 1}{2}$$
$$f(x_2) = \frac{x_2 + 1}{2}$$

and since $x_1 \neq x_2$ it follows that

$$\frac{x_1 + 1}{2} \neq \frac{x_2 + 1}{2}$$

and so

$$\implies f(x_1) \neq f(x_2)$$

and so we are done.
Case III: (x_1, x_2 are both even): In this case,

$$f(x_1) = \frac{-x_1}{2}$$
$$f(x_2) = \frac{-x_2}{2}$$

and since $x_1 \neq x_2$ it follows that

$$\frac{-x_1}{2} \neq \frac{-x_2}{2}$$

and so

$$\implies f(x_1) \neq f(x_2)$$

and so we are done.

This shows that f is injective. We will now show that f is surjective. Let $y \in \mathbb{Z}$ be an arbitrary integer.
Case I ($y > 0$): In this case consider $x = 2y - 1$. Clearly, if $y > 0$ then $x = 2y - 1 > 0$, and so $x \in \mathbb{N}$ which is the domain of f. Also $x = 2y - 1$ is odd so we have that

$$f(x) = f(2y - 1) = \frac{2y - 1 + 1}{2} = y,$$

and so we have found an x such that $f(x) = y$.
Case II ($y \leq 0$): In this case consider $x = -2y$. Clearly, if $y \leq 0$ then $x = -2y \geq 0$, and so $x \in \mathbb{N}$ which is the domain of f. Also $x = -2y$ is even so we have that

$$f(x) = f(-2y) = -\frac{-2y}{2} = y,$$

and so we have found an x such that $f(x) = y$.

This proves that f is surjective. Combining the facts that f is injective and surjective, we can conclude that f is bijective and this shows that $\mathbb{Z}$ is countably infinite and hence

$$|\mathbb{Z}| = \aleph_0.$$

□

There is another term that is used frequently in mathematics.

Definition 4. If a set S is finite or countably infinite then we say that the set is *countable*.

Infinite sequences

We talked about finite sequences a couple of lectures ago; basically, an n-tuple is a finite sequence. For example, $(1, 2, 4, 5)$ is a finite sequence. We can also choose to write it as $1, 2, 4, 5$ or say that the sequence is a_0, a_1, a_2, a_3 where

$$a_0 = 1, a_1 = 2, a_2 = 4, a_3 = 5.$$

This idea can be easily generalized to infinite sequences. Consider the following infinite sequence:

$$1, 3, 5, 7, 9, \ldots,$$

i.e. the sequence $a_0, a_1, \ldots, a_n, \ldots$ where

$$a_n = 2n + 1.$$

So infinite sequences "assign" a value to each "position". Note that a_0 is in the first position and not a_1 (a_1 is in the second position). In the above example, the infinite sequence assigns the value $2n+1$ to the $(n+1)^{th}$ position: a_0, the first position, is assigned the value 1, a_1, the second position, is given the value 3, a_2, the third position, is assigned the value 5, and so on.

Consider another infinite sequence

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$$

Here $a_0 = 1$, $a_1 = \frac{1}{2}$, $a_2 = \frac{1}{3}$, and so on. Thus, this infinite sequence assigns the value 1 to a_0 (the first position), $\frac{1}{2}$ to a_1 (the second position), and so on, and so we can say that it assigns the value

$$\frac{1}{n+1}$$

to a_n (i.e., the $(n+1)^{th}$ position).

Note that sometimes some people prefer to start sequences with a_1 instead of a_0. This doesn't change much; instead of a_n appearing at the $(n+1)^{th}$ position, it now appears at the n^{th} position. So, the first example we saw, i.e. $1, 3, 5, 7, \ldots$ can also be written as $a_1, a_2, \ldots, a_n \ldots$ where

$$a_n = 2n - 1, \text{ for } n \geq 1.$$

(Recall that if we start with a_0 then $a_n = 2n + 1$). We will always start sequences with a_0.

Another thing to remember is that it is possible for the same value to appear at many different positions in an infinite sequence. For example, consider the sequence,

$$1, -1, 1, -1, 1, -1, \ldots$$

in which $a_n = 1$ for all even values of n, and $a_n = -1$ for all odd value of n. Clearly, this sequence has repeating values.

Some infinite sequences have a "pattern" to them and so can be described using a mathematical formula/expression. For example, the infinite series $1, \frac{1}{2}, \frac{1}{3}, \ldots$ can be described by the formula

$$a_n = \frac{1}{n+1}, \text{ for } n \geq 0.$$

Sometimes, instead of directly giving a formula for a_n, it's easier to describe what the first few terms of the infinite sequence are, along with how a_n can be computed from $a_0, a_1, \ldots, a_{n-1}$. Such descriptions are called *recurrences* or *recursive definitions.*

For example, consider the following recurrence:

$$a_0 = 0, a_1 = 1$$

$$a_n = a_{n-1} + a_{n-2} \text{ for } n \geq 2.$$

We can use the information provided above to compute the next few terms of the sequence:

$$a_2 = a_1 + a_0 = 1 + 0 = 1$$

$$a_3 = a_2 + a_1 = 1 + 1 = 2$$

$$a_4 = a_3 + a_2 = 2 + 1 = 3$$

and so on. This is the famous *Fibonacci sequence.* It turns out that it's easier to describe the Fibonacci sequence using a recurrence/recursive definition instead of directly giving a formula for a_n (the $(n+1)^{th}$ term of the sequence). The latter turns out to be slightly more complicated and we wouldn't get into that here.

Of course, not all sequences can be described using a nice formula or a recurrence. For example, if we create a sequence from the digits of π after the decimal point, i.e.

$$1, 4, 1, 5, 9, 2, \ldots,$$

where $a_0 = 1$ and so on, we do not know how to describe a_n using a formula/recurrence. In fact, it is believed that it is not possible to do so but we will not discuss that here.

We can use induction to prove interesting things about sequences that can be described using recurrences.

Problem 3. Let $a_0, a_1, \ldots, a_n \ldots$ be the Fibonacci sequence. Prove that for all $n \geq 0$

$$\sum_{i=0}^{n} a_i^2 = a_0^2 + \ldots + a_n^2 = a_n \cdot a_{n+1}.$$

Proof. We can use weak induction to prove this statement. Let $P(n)$ be the statement that

$$a_0^2 + \ldots + a_n^2 = a_n \cdot a_{n+1}.$$

We want to prove $\forall n \geq 0 \; P(n)$.
Base case: $P(0)$ is the statement

$$a_0^2 = a_0 \cdot a_1.$$

This is easy to see: $a_0 = 0$ and so a_0^2 is 0, and also $a_0 \cdot a_1 = 0$ and so $P(0)$ is true.
Induction step: We will now prove that

$$\forall n \geq 0 \; P(n) \rightarrow P(n+1).$$

Let $k \geq 0$ be an arbitrary number. It suffices to show that $P(k) \rightarrow P(k+1)$.
Let us assume that $P(k)$ is true, i.e.

$$a_0^2 + \ldots + a_k^2 = a_k \cdot a_{k+1}.$$

This is our induction hypothesis. We will now try to use this to prove that $P(k+1)$ is true, i.e.

$$a_0^2 + \ldots + a_{k+1}^2 = a_{k+1} \cdot a_{k+2}.$$

Let us begin with the left hand side of the above expression:

$$a_0^2 + \ldots + a_{k+1}^2$$

$$= (a_0^2 + \ldots + a_k^2) + a_{k+1}^2$$

Using the induction hypothesis in the above expression, (i.e., $a_0^2 + \ldots + a_k^2 = a_k \cdot a_{k+1}$) we get

$$= a_k \cdot a_{k+1} + a_{k+1}^2$$

$$= a_{k+1} \left(a_k + a_{k+1}\right) \quad (1)$$

Now remember that for all $n \geq 2$ the Fibonacci sequence has the following recurrence:

$$a_n = a_{n-1} + a_{n-2}$$

Since $k \geq 0$, we have that $k + 2 \geq 2$, and so

$$a_{k+2} = a_{k+1} + a_k$$

We can use this equality in Equation (1) to conclude that

$$a_0^2 + \ldots + a_{k+1}^2 = a_{k+1} \left(a_k + a_{k+1}\right)$$

$$= a_{k+1} \cdot a_{k+2}.$$

This completes the inductive proof. $\square$

Infinite sequences and countable sets

Why did we introduce infinite sequences at all? It's because of the following nice fact that can let us argue that a set S is countably infinite:

Fact 5. Let S be an infinite set. Then S is countably infinite if and only if there is an infinite sequence $a_0, a_1, \ldots, a_n \ldots$ such that

1. the sequence only contains elements from S, i.e.

$$\forall n \in \mathbb{N} \; a_n \in S.$$

2. every element of S appears *at least once* in the sequence, at some position. More formally, for every $s \in S$ there is some $i \in \mathbb{N}$ such that

$$a_i = s,$$

   i.e. s appears in the $(i+1)^{th}$ position.

We will prove this fact in a later section.

This fact affords us a very intuitive way of proving a set S is countably infinite: construct an infinite sequence in which all the elements of S appear at least once, and no other elements appear. In other words, propose a way to "arrange" the elements of S into an infinite sequence.

We will now use the above show that the union of two countable sets is also countable.

Fact 7. Let A and B be countable sets. Then $A \cup B$ is also countable.

Proof. **Case I (Both A and B are finite):** This is the easy case: $A \cup B$ is clearly going to be finite and thus countable.
Case II (A is finite or B is finite, but not both): Without loss of generality, assume that A is finite, and suppose that

$$A = \{a_0, \ldots, a_k\}.$$

Now since B is countable but not finite, it must be countably infinite, and so using Fact 5, there is an infinite sequence $b_0, b_1, \ldots,$ such that every element of B appears at least once in the sequence, and only elements from the set B appear in the sequence.

Let us define a new infinite sequence $c_0, c_1, \ldots$ as follows:

- For $0 \leq n \leq k$, $c_n = a_n$, and
- for $n > k$, $c_n = b_{n-k-1}$.

In other words, $c_0, c_1, \ldots$ is the following infinite sequence

$$a_0, a_1, \ldots, a_k, b_0, b_1, \ldots$$

It is easy to see that the sequence $c_0, c_1, \ldots$ only contains elements from $A \cup B$, and every element from $A \cup B$ appears at least once in the sequence. Thus, using Fact 5, $A \cup B$ must be countably infinite.
Case III (Both A and B are infinite): In particular, both A and B are countably infinite, and so using Fact 5, there are sequences $a_0, a_1, \ldots$ and $b_0, b_1, \ldots$ such that

- Every element of A appears at least once in the first sequence, and only elements of A appear in that sequence.
- Every element of B appears at least once in the second sequence, and only elements of B appear in that sequence.

Let us use these sequences to define a new sequence $c_0, c_1, \ldots$ as follows:

- For all even values of $n \in \mathbb{N}$, $c_n = a_{\frac{n}{2}}$, and
- for all odd values of $n \in \mathbb{N}$, $c_n = b_{\frac{n-1}{2}}$.

Basically, the sequence $c_0, c_1, \ldots$ looks like

$$a_0, b_0, a_1, b_1, \ldots$$

Again, it's not hard to see that every element of $A \cup B$ appears at least once in the sequence, and only elements from $A \cup B$ appear in the sequence. Thus, using Fact 5, $A \cup B$ is countable. $\square$

Sets generated by algorithms/procedures

Definition 5. A procedure/algorithm A is said to generate a set S if

1. A only prints elements from S and nothing else, and
2. every $s \in S$ is printed at least once by A.

Clearly, any procedure/algorithm for printing an infinite set must have an infinite loop inside it. We can now combine Fact 5 and Definition 5 to conclude the following very useful fact

Fact 7. If there is a procedure/algorithm that generates an infinite set S, then S must be countably infinite.

Proof. Define the following sequence $a_0, a_1, \ldots$ using A:

$$a_n = \text{the } (n+1)^{th} \text{ value printed by } A.$$

Then it is not hard to see that every element of s appears at least once in the sequence, and nothing but elements of S appear in it. Thus, using Fact 5, S must be countably infinite. $\square$

Thus, to show that a set S is countably infinite, all you need to do is to describe a procedure/algorithm that prints out elements of S. Let us use this idea to show that $\mathbb{N} \times \mathbb{N}$ is countably infinite.

Fact 8. $\mathbb{N} \times \mathbb{N}$ is countably infinite.

Proof. We will describe a procedure to generate $\mathbb{N} \times \mathbb{N}$.

- Loop i over all natural numbers, starting with 0, and incrementing by 1 every time.
- Inside the loop, for every i, do the following: print all pairs $(a, b) \in \mathbb{N} \times \mathbb{N}$ such that $a + b = i$. There are exactly i such pairs and it is easy to write a procedure to print all such pairs exactly once: loop over all values $j \in \{0, 1, \ldots, i\}$, and in every iteration print $(j, i - j)$.

For $i = 0$, the procedure will only print $(0, 0)$, for $i = 1$, it will print $(0, 1)$ and $(1, 0)$, for $i = 2$, $(0, 2), (1, 1), (2, 0)$, and so on. It is not hard to see that every $(a, b) \in \mathbb{N} \times \mathbb{N}$ is printed at least once, and nothing but values from $\mathbb{N} \times \mathbb{N}$ are printed. Thus, using Fact 7, $\mathbb{N} \times \mathbb{N}$ is countable. $\square$

Subsets of countable sets

Our goal is to show that subsets of countable sets are also countable.

Fact 9. Let S be a countable set. Then for every $T \subseteq S$, T is countable.

We will discuss the proof of this fact in Part II of the notes.