Lecture notes on cardinality and infinite sets (Part II)

Notation for sequences

So far we have been denoting sequences by a_0, a_1, \ldots A more compact and easier way to write this is $\{a_n\}$. This basically is a short-hand for saying "the infinite sequence a_0, a_1, a_2, \ldots ". So instead of saying "Let a_0, a_1, \ldots be an infinite sequence" we can say "Let $\{a_n\}$ be a sequence". Similarly we can use $\{b_n\}$ to denote b_0, b_1, \ldots and $\{c_n\}$ to denote c_0, c_1, \ldots

Guessing formulas for sequences

Sometimes sequences are described using recurrences but we want to come up with an explicit formula for each term using the recurrence. For example, consider the sequence $\{a_n\}$ given the recurrence

$$a_0 = 1$$

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

We want to a find a *closed-form formula* for a_n . By that I mean a formula for a_n purely in terms of n (i.e., something like n^2 or 2n + 3, or $n^3 + 2n^3$, etc.).

One way of doing this is to first compute a few terms of the sequence and then try to observe a pattern to guess a formula. Let's compute the first few terms using the above recurrence.

$$a_1 = 2 \times a_0 = 2$$

$$a_2 = 2 \times a_1 = 4$$

$$a_3 = 2 \times a_2 = 8$$

and so on. If you stare at these values a bit, you can easily guess that the formula should be $a_n = 2^n$ for $n \ge 0$. But we just have a guess for the formula so far. To formally show that this is indeed the right formula, we need to use induction. Let P(n) be the predicate

"
$$a_n = 2^n$$
"

Our goal is to prove that $\forall n \geq 0 \ P(n)$.

Base case: This is the case when n = 0. Well, a_0 is given to be 1 and also $2^0 = 1$, so we have that

$$a_0 = 2^0$$

and so P(n) is true for n=0.

Induction step: We now want to show that $\forall n \geq 0 \ P(n) \rightarrow P(n+1)$. Let $k \geq 0$ be an arbitrary number. It suffices to prove that $P(k) \rightarrow P(k+1)$.

Let us assume P(k) is true, i.e

$$a_k = 2^k$$
.

This is the induction hypothesis. Our goal is to show that P(k+1) is true, i.e. $a_{k+1} = 2^{k+1}$. The recurrence saying that $\forall n \geq 1$

$$a_n = 2 \cdot a_{n-1}.$$

Since $k \geq 0$, $k+1 \geq 1$, and so we can applying the recurrence for a_{k+1} to get

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

Since $a_k = 2^k$ using the induction hypothesis, we get

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

and this finishes the proof.

Cartesian products of countable sets

In Part I of the notes we showed that $\mathbb{N} \times \mathbb{N}$ is countably infinite (See Fact 8 in Part I). Let us use that to show that if A, B are countable then $A \times B$ is countable.

Fact 10. If A and B are countable, then so is $A \times B$.

Proof. We will do a case analysis:

Case I (A and B are both finite): In this case $A \times B$ is finite and so it is also countable by definition.

Case II (Either A or B is finite, but not both): Without loss of generality (and via symmetry), assume that A is finite but B is countably infinite. Let us assume that |A| = k and so

$$A = \{a_1, \dots, a_k\}.$$

Also, since B is countably infinite, we can use Fact 5 to conclude that there is some sequence

$$b_0, b_1, \dots$$

such that only elements of B appear in the sequence and also every element of B appears in the sequence at least once.

We will now write pseudocode for a procedure/algorithm that will print elements of the set $A \times B$:

- Loop i over all natural numbers, starting at 0 and incrementing by 1 in every iteration.
- Inside the outer loop, there is another loop that has a variable j that loops from j = 1 to j = k.
- Inside the inner loop (the one with j as the loop variable), we simply print the element (a_j, b_i) of $A \times B$.

It is not hard to see that this procedure only prints elements of $A \times B$ and every element of $A \times B$ is printed at least once.

Case III (Both A and B are countably infinite): If both A and B are countably infinite then there are bijections

$$g:A\to\mathbb{N}$$

and

$$h: B \to \mathbb{N}$$
.

We can use these functions to define a bijection

$$f: A \times B \to \mathbb{N} \times \mathbb{N}$$

as follows

$$f(a,b) = (g(a), h(b)).$$

To see that f is surjective, let $(i,j) \in \mathbb{N} \times \mathbb{N}$ be some arbitrary element. Then if we take

$$(a,b) = (g^{-1}(i), h^{-1}(j))$$

then

$$f(a,b) = (g(g^{-1}(i)), h(h^{-1}(j))) = (i, j).$$

This shows that every element in $\mathbb{N} \times \mathbb{N}$ is in the range of f and so f is surjective.

To see that f is injective, let (a,b) and (a',b') be two distinct elements of $A \times B$. Then we have the following from the definition of $(a,b) \neq (a',b')$,

$$(a,b) \neq (a',b')$$

$$\Rightarrow (a \neq a') \lor (b \neq b').$$

Suppose that $a \neq a'$. In that case, since g is injective, we have that

$$g(a) \neq g(a')$$

and so

$$f(a,b) = (g(a), h(b)) \neq (g(a'), h(b')) = f(a', b').$$

Similarly, if a = a' but $b \neq b'$, then we can use the injectivity of h to conclude that

$$h(b) \neq h(b')$$

and so

$$f(a,b) = (g(a),h(b)) \neq (g(a'),h(b')) = f(a',b').$$

Thus, f is injective.

This means f is bijection. Also, recall that we proved (in Fact 8, Part I) that $\mathbb{N} \times \mathbb{N}$ is countably infinite and so there must be a bijection $f': \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. We can then combine the two bijections $f: A \times B \to \mathbb{N} \times \mathbb{N}$ and $f': \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ using composition to get the function

$$(f' \circ f) : A \times B \to \mathbb{N}$$

which is also a bijection (See Problem 2 (Part 1) on HW 4), and so $A \times B$ is countably infinite. \square

Subsets of countable sets

Before we prove that subsets of countably sets are also countably (a rather intuitive fact), we will prove the following obvious but important fact (also known as the "well-ordering principle"):

Fact 11. Every non-empty subset S of the natural numbers \mathbb{N} has a unique minimum element.

Proof. We did an informal proof in the class. Here we will give a formal proof using induction.

Note that the "unique" part just follows easily from the definition of sets (since they can't have duplicates) and the strict ordering of the natural numbers (no two natural numbers are equal to each other) if we can show that there is a minimum element in every non-empty set. We can think of the statement as a conditional:

"If S is not empty then S has a minimum element".

We can consider the contrapositive of this statement:

"If S has no minimum element then S is the empty set.".

We will prove the contrapositive using strong induction. Let S be any arbitrary subset of the natural numbers such that S has no minimum element. Our goal is to show that $S = \emptyset$ which is equivalent to the following statement

$$\forall k \geq 0 \ k \notin S$$
.

Let P(k) be the predicate

$$k \notin S$$
,

and so we want to prove that

$$\forall k > 0 \ P(k)$$
.

Base case: We want to prove that P(0) is true, i.e. $0 \notin S$. Suppose for the sake of contradiction that $0 \in S$, then 0 will be the minimum element of S since all other natural numbers that S may contain will be larger than 0. This would be a contradiction since we assumed S to be a set that has no minimum element. Thus, $0 \notin S$ and so P(0) is true.

Induction step: We will prove that for all $k \geq 0$

$$(P(0) \wedge P(1) \wedge \dots P(k)) \rightarrow P(k+1).$$

Let $k \ge 0$ be an arbitrary natural number and suppose $(P(0) \land P(1) \land \dots P(k))$ is true. It suffices to prove that P(k+1) is true to prove the general statement for all $k \ge 0$.

Since k is such that $P(0), P(1), \ldots, P(k)$ are all true, this means that for all $0 \le j \le k$, j is not contained in S, i.e. $j \notin S$. This is our induction hypothesis.

Our goal is to show that P(k+1) is true, i.e. k+1 is also not contained in S. This is easy to prove using contradiction: suppose $k+1 \in S$ then since none of the numbers less than k+1 are in S (because of the induction hypothesis) that would make k+1 the minimum element, which would contradict the fact that S does not have a minimum element. Thus, k+1 cannot be in S and so P(k+1) is true.

This completes our induction proof and establishes that

$$\forall k \geq 0 \ k \notin S$$

which is logically equivalent to saying $S = \emptyset$ and so we have proved the contrapositive.

For infinite subsets of the natural numbers, we can easily extend the above fact to the following:

Fact 12. Let S be an infinite subset of the natural numbers. Then, for every $i \ge 1$, S has a unique i^{th} smallest element.

Proof. We will prove this using strong induction. Let S be an aribtrary infinite subset of \mathbb{N} . Let P(i) be following predicate

"S has a unique i^{th} smallest element.".

Our goal is to prove that

$$\forall i \geq 1 \ P(i)$$
.

Base case: The fact that P(1) is true (i.e., S has a unique 1^{st} smallest (i.e., minimum) element) follows from Fact 11.

Induction step: Let $i \geq 1$ be an arbitrary natural number. Our goal is to prove that

$$P(1) \wedge P(2) \wedge \ldots \wedge P(i) \rightarrow P(i+1).$$

Suppose now that $P(1), P(2), \ldots, P(i)$ are all true, i.e. S contains a unique j^{th} smallest element for all $1 \le j \le i$. This is the induction hypothesis. We now show that P(i+1) is true.

Let S(j) denote the unique j^{th} smallest element of S for $1 \leq j \leq i$ (these exist because of the induction hypothesis), and define the set

$$S' := \{S(j) | 1 \le j \le i\}$$

i.e. the set of the first i smallest elements. Clearly, S' is finite, and so the set S - S' is still infinite since deleting a finite number of elements from an infinite set will not make it into a finite set. Since S - S' is an infinite subset of \mathbb{N} we can apply Fact 11 to conclude that it has a unique minimum element, say s. From the way we defined S', it should be clear that there are only i element in S that are strictly smaller than s, and so s is the unique $(i+1)^{th}$ smallest element in S, and this proves P(i+1).

We will now use the above fact to show that every subset of $\mathbb N$ is countable

Fact 13. Every subset $T \subseteq \mathbb{N}$ is countable.

Proof. Let $T \subseteq S$. There are two cases:

Case 1 (T is finite): If T is finite then it is countable and so there is nothing to prove here.

Case 2 (T is infinite): Let us define a bijection $f: \mathbb{N} \to T$ as follows: for $n \geq 0$,

$$f(n) =$$
 "The $(n+1)^{th}$ smallest element of T ".

From Fact 12, we know that for every $n \geq 0$ the $(n+1)^{th}$ smallest element of T is uniquely1-defined since T is an infite set, and hence the function f is correctly defined (this just means that f transforms every $n \in \mathbb{N}$ into exactly one element in T).

Clearly f is injective because a set cannot contain duplicate values and so there are no ties and hence for every $i, j \in \mathbb{N}$ such that $i \neq j$, the $(i+1)^{th}$ smallest element of T is going to be different from the $(j+1)^{th}$ smallest element of T, which in turn implies that $f(i) \neq f(j)$.

We will now argue why f is also surjective and this will finish the proof since it will imply that f is a bijection. Let $t \in T$ be an arbitrary element. Since T is an infinite set it has a minimum element by Fact 12. Let us call this minimum element m. If m = t then f(1) = m = t and so t would be in Range(f). Otherwise, m < t. Now, obviously, there are finitely many natural numbers between the natural numbers m and t, and so, the set

$$T' = \{x \in T | m \le x \le t - 1\}$$

is also finite. Let us assume that |T'| = k. Note that $T' \subset T$ and also that T - T' is infinite since T is infinite and T' is finite. Using Fact 12, we can conclude that T - T' must have a unique minimum element m'. Also, the only elements of T that are smaller than m' are those elements that are contained in T', and so m' is the $(k+1)^{th}$ smallest element of T (since |T'| = k). Thus, f(k) = m'.

We will now argue that m' is in fact equal to t and then that would imply that f(k) = t and complete the proof. Suppose $m' \neq t$. There are two cases to consider and both cases lead to a contradiction:

Case 1 (m' < t, or in other words $m' \le t - 1$): If $m' \le t - 1$ then since $m' \in T$ it would have been included in the set T' by definition and could not have been present in the set T - T', which would contradict the fact that m' is the unique minimum element of T - T'.

Case 2 (t < m'): The way we defined T', it is clear that t is not contained in T'. This means that $t \in T - T'$. We have that t < m' which would mean that t is an element of T - T' that is smaller than m' which is the unique minimum of T - T' leading to a contradiction.

Thus, since both possibilities lead to a contradiction, our assumption that $m' \neq t$ is wrong, and so

$$t = m' = f(k)$$

and this shows that t is in Range(f). Thus, since t was an aribtrary element of the codomain in the above proof, it follows that f is surjective and hence bijective.

We will now prove another fact that will help to prove the main result of this section that every subset of a countable set is also countable.

Fact 14. Let $f: A \to B$ be any injective function. Then there is a bijection between A and Range(f).

Proof. This is an easy proof. Let us define the function $g: A \to Range(f)$ and then show that g is a bijection. g is defined as: for every $a \in A$

$$g(a) = f(a).$$

Cleary, g is injective because f is injective. Also, if $b \in Range(f)$ is an arbitrary point then by the very definition of Range(f) there must be an $a \in A$ such that f(a) = b, and then this would imply that g(a) = f(a) = b. This means that Range(g) = Range(f) and so g is also surjective. Hence, g is a bijection.

We will now use this to prove the main result of this section:

Fact 15. Let S be a countable set. Then every $T \subseteq S$ is also countable.

Let $T \subseteq S$ be an arbitrary set. There are two cases:

Case I (T is finite): If T is finite, then T is countable by definition.

Case II (T is infinite): If T is infinite then S is also infinite since $T \subseteq S$. Furthermore, since S is countable and also infinite, it follows that S is countably infinite. This means there is a bijection $f: S \to \mathbb{N}$.

Let us define a new function $g: T \to \mathbb{N}$ as follows

$$g(t) = f(t)$$
.

Then, since f is injective, g is also injective. Using Fact 14, we can conclude that there is a bijection between T and Range(g). Note that Range(g) is a subset of the natural numbers and thus using Fact 13, Range(g) is countable. Also, since T is infinite, it must be the case that Range(g) is infinite, otherwise there cannot be a bijection between them. Thus, since Range(g) is countably and infinite, it must be countably infinite. We can now use Part 2 of Problem 2 on HW 4 to conclude that T is also countably infinite.

Back to proving the sequence lemma

Recall Fact 5 from Part I of the notes (which we call the "sequence lemma" from now on) which we stated but did not prove. We will prove it now:

Fact 5 (The sequence lemma). Let S be an infinite set. Then S is countably infinite if and only if there is an infinite sequence $\{a_n\}$ 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.

Proof.

Let S be an infinite set. Let us first prove the "only if" part of the statement, i.e. if S is countably infinite then there is a sequence $\{a_n\}$ with the desired properties. If S is countably infinite there is a bijection $f: \mathbb{N} \to S$. We can define a sequence $\{a_n\}$ as follows: for every $n \ge 0$

$$a_n = f(n)$$
.

Clearly, for all $n \in \mathbb{N}$, $a_n \in s$, and also every s appears once in the sequence: let $s \in S$ be arbitrary then since f is a bijection there is an $i = f^{-1}(s)$ such that f(i) = s, and so $a_i = s$.

Let us now prove the other direction, i.e. if there is a sequence with $\{a_n\}$ such that $\forall n \in \mathbb{N}$ $a_n \in S$, and $\forall s \in S$ there is some $n \in \mathbb{N}$ such that $a_n = s$, then S is countably infinite. Let us define a function $f: \mathbb{S} \to \mathbb{N}$ as follows: let $s \in S$ be arbitrary

• Let N_s the set of all positions in the sequence $\{a_n\}$ where s appears, i.e.

$$N_s = \{ i \in \mathbb{N} | \ a_i = s \}.$$

- Clearly, $N_s \subseteq \mathbb{N}$ and since every element appears in the sequence at least once we can also conclude that $N_s \neq \emptyset$. Thus, using Fact 11, N_s has a unique minimum element, say m.
- We will define

$$f(s) = m,$$

in other words, f(s) is the first position in the sequence $\{a_n\}$ at which s appears.

It is easy to see that f is injective: two elements cannot appear for the first time at the same position since exactly once element of S is associated with each position in the sequence. Using Fact 14, there is a bijection between S and Range(f). Since Range(f) is an infinite subset of \mathbb{N} , it follows from Fact 13 that Range(f) is countably infinite. Again, using Part 2 of Problem 2 on HW 4, it follows that S is also countably infinite.

The effect of other set operations on the cardinality of infinite sets

So far we have shown that both the union and cartesian product of two countable sets is countable. We will now state some facts about other set operations without proof (the proofs are super easy if you use Fact 15 and you should try them as an exercise):

Fact 16. If A, B are countable sets then $A \cap B$ is also countable.

Fact 17. If A, B are countable sets then A - B and B - A are also countable.

Fact 18. If A, B are countable sets then $A \oplus B$ is also countable.

We still haven't talked about one set operation: $pow(\cdot)$.

Powersets of countably infinite sets and uncountability

We will introduce some more definitions before we prove some interesting things about powersets of countably infinite sets.

Definition 19. For two infinite sets A and B, we say that $|A| \leq |B|$ if there is an injective function $f: A \to B$.

Recall that for finite sets $|A| \leq |B|$ simply means that B has more elements than A. The above definition of $|A| \leq |B|$ for infinite sets A, B also implies something similar, at least in an informal and intuitive sense. If there is an injective function $f: A \to B$ then that means that it is possible to find a unique "partner" in B for every element of A in a way that no two elements of A have the same "partner" in B. Intuitively speaking, this means that B has at least as many elements as A. Similarly, we can also define $|A| \geq |B|$ using surjective functions:

Definition 20. For two infinite sets A and B, we say that $|A| \ge |B|$ if there is a surjective function $f: A \to B$.

Again, intuitively speaking, this definition implies that A has "more elements" than B. Think of the elements of A as customers, and elements of B as shops, and f(a) = b means that a visits shop b. Since f is a function, it means that every customer visits exactly one shop. Since f is surjective, it means that every shop in B received at least one customer from A which would only be possible if there were more customers than shops (since a single customer can visit only one shop).

We will first consider the powerset of natural numbers, i.e. $pow(\mathbb{N})$. Recall that this is the set of all possible subsets of \mathbb{N} . Note that this set is infinite since the following (infinitely many) elements are members of this set:

$$\{1\}, \{2\}, \{3\}, \{4\}, \dots$$

Basically, for every $i \in \mathbb{N}$, the singleton set that contains only the number i, i.e. $\{i\}$, is in the powerset of \mathbb{N} . The question is whether pow(\mathbb{N}) contains "more elements" than \mathbb{N} . It turns out it does!

Fact 20. The power set of the natural numbers, i.e. $pow(\mathbb{N})$, is not countably infinite, i.e. it is not possible to define a bijection between \mathbb{N} and $pow(\mathbb{N})$.

Proof. We will prove this statement by contradiction. Suppose for the sake of contradiction that $pow(\mathbb{N})$ is countably infinite and so there is a bijection $f: \mathbb{N} \to pow(\mathbb{N})$. Note that here, for every $n \in \mathbb{N}$, $f(n) \in pow(\mathbb{N})$ is some subset of \mathbb{N} .

We will now define a set $S \subseteq \mathbb{N}$ using f as follows: for every $n \in \mathbb{N}$, n is in the set S if and only if n is not in the set f(n), i.e.

$$n \in S \leftrightarrow n \notin f(n)$$
.

It is clear that $S \subseteq \mathbb{N}$ and so it follows that $S \in \text{pow}(\mathbb{N})$. This means that S is in the codomain of f. Since f is a bijection, it is also surjective, and so there must be some $j \in \mathbb{N}$ such that f(j) = S. We will now show that there are two possibilities here, both of which lead to a contradiction:

Case I $(j \in f(j))$: If j is contained in the set f(j) then j will not be in the set S because of how set S is defined. Then since $j \in f(j)$ and $j \notin S$, it must be the case that $f(j) \neq S$, a contradiction. Case II $(j \notin f(j))$: If j is not contained in the set f(j) then j will be contained in the set S because of how set S is defined. Then since $j \notin f(j)$ and $j \in S$, it must be the case that $f(j) \neq S$, a contradiction.

Since $j \in f(j)$ and $j \notin f(j)$ are the only possibilities, and both lead to a contradiction, our initial assumption that f is a bijection must be false, and so there cannot be any bijection between \mathbb{N} and pow(\mathbb{N}).

This means that there is another "type" of infinity, different from countable infinity, and also "larger" than countable infinity. Recall that $|\mathbb{N}| = \aleph_0$. Similarly, we say that $|\text{pow}(\mathbb{N})| = \aleph_1$ and as demonstrated \aleph_1 represents a "larger" infinity than \aleph_0 . A set whose cardinality is larger than that of \mathbb{N} are called *uncountable sets*.

Definition 21. Let S be an infinite set such that there is no bijection between \mathbb{N} and S (i.e., S is not countably infinite). Then S is called an *uncountable set*.

We can now state a general fact about the power sets of countably infinite sets that directly follows from Fact 20.

Fact 22. Let S be a countably infinite set then pow(S) is uncountable.

Proof. We will prove this by contradiction. Suppose there is a countably infinite set S such that pow(S) is also countably infinite. Since S is countably infinite there is a bijection $f: \mathbb{N} \to S$. We will now use f to define a bijection between $pow(\mathbb{N})$ and pow(S).

Let $g : pow(\mathbb{N}) \to pow(S)$ be a function defined as follows: for a set $X \in pow(\mathbb{N})$,

$$g(X) = \{ f(i) | i \in X \}.$$

Clearly, for every $X \in \text{pow}(\mathbb{N})$, $g(X) \in \text{pow}(S)$. Furthermore, it is not hard to see that since f is a bijection, g is also a bijection (Try thinking about this!). Now since $\text{pow}(\mathbb{N})$ and pow(S) have a bijection between them, and pow(S) is countably infinite, it follows from Part 2 of Problem 2 on HW 4 that $\text{pow}(\mathbb{N})$ is also countably infinite, which is a contradiction to Fact 20. Thus, our assumption that there is a set S that is countably infinite whose powerset is also countably infinite must be false, and so the powerset of every countably infinite set is uncountable.

The cardinalities of the rational, irrational, and real numbers

We will not prove some of the facts we state in this section. However, these are facts you should know, and we *might* have problems that will guide you through a proof of these facts.

Fact 23. The set of rational numbers \mathbb{Q} is countably infinite.

One can use the countability of $\mathbb{N} \times \mathbb{N}$ to prove this.

Fact 24. The set of real numbers \mathbb{R} is uncountable.

This fact is not that easy to prove but intuitively it makes sense: if you think about it, it doesn't seem like there should be a bijection between \mathbb{N} and \mathbb{R} . We can combine the two facts to conclude something interesting:

Fact 25. The set of irrational numbers is uncountable.

Proof. We will prove this by contradiction. Let \mathbb{I} denote the set of irrational numbers. Suppose for the sake of contradiction that \mathbb{I} is a countable set. Since every real number is either rational or irrational, we can say that

$$\mathbb{R} = \mathbb{I} \cup \mathbb{O}$$
.

Since \mathbb{Q} is countable (via Fact 23), and \mathbb{I} is also countable (our assumption), Fact 7 from Part I of the notes implies that $\mathbb{I} \cup \mathbb{Q}$ must also be countable, and so \mathbb{R} is countable, which is a contradiction to Fact 24. Thus, our assumption that \mathbb{I} is countable is false, and it must be the case that \mathbb{I} is uncountable.