Michael A. Bender

CSE 150 Foundations of Computer Science: Honors, Fall 2005

Assignment #2

Aleph-null bottles of beer on the wall,
Aleph-null bottles of beer on the wall,
Take one bottle down and pass it around
Aleph-null bottles of beer on the wall.
-a folk song

The goal of this homework is to improve your formal proof techniques and give you more insights on the issues of countability. The first excercise is solved for you as an example. Some theorems might follow directly from theorems that appear before them, in such case you just need to write out what follows from what.

Excercise 1:
Show that the epigraph is true in the mathematical sense, i.e. $|\mathbb{N}| = |\mathbb{N} - \{1\}|$

Proof:
Let $X = |\mathbb{N} - \{1\}|$. We show that $|X| = |\mathbb{N}|$ by demonstraing a bijection between these sets. Let $f : X \rightarrow \mathbb{N}$ be defined as follows: $f(n) = n - 1$. We claim that f is bijective. First observe that f is injective. Indeed, let $f(a) = f(b)$ for some $a, b \in X$. Then $a - 1 = b - 1$ and $a = b$. Note that f is also surjective: $\forall a \in \mathbb{N} : \exists b = a + 1$ such that $f(b) = a$ and $b \in X$. Indeed, $f(b) = f(a + 1) = a + 1 - 1 = a$; also $a \in \mathbb{N} \Rightarrow a \geq 1 \Rightarrow a + 1 \geq 2$; hence $a + 1 = b \in X$. $\square$

Note: For any set X, if $|X| = |\mathbb{N}|$, we are granted that a bijection $\phi : \mathbb{N} \Rightarrow X$ exists. We can use $\phi(n)$ to obtain the element in X that corresponds to n, and use $\phi^{-1}(x)$ to get the number that x corresponds to.

Observe that X was a subset of N, and since it didn't include 1, it was a proper subset. When can a cardinality of a proper subset be the same as cardinality of its superset ? In what cases does it happen ? We shall explore it in the following excercises. Bonus points will be awarded for theorems labeled as "Bonus"'.

First, prove what is almost clear from Excercise 1:

Proposition 1.1
$|\mathbb{N}| = |\mathbb{N} - A|$, where $A = \{1, 2, 3, ..., k\}$

Now let's explore what happens if you take an infinite number of elements out of $\mathbb{N}$. Let's take out all the odd numbers. Prove or disprove the following:

Proposition 1.2
The even positive integers have the same cardinality as the natural numbers.

If you thought that the previous proposition was true and proved it, you might have asked yourself if it is the case in general.

Bonus Theorem 1.3
Every subset of $\mathbb{N}$ is either finite or has the same cardinality as $\mathbb{N}$.

Hint: Use the fact that any nonempty set of positive integers has a least element. If X is a subset of $\mathbb{N}$, show that $f(n) = min\{X - \bigcup_{i=1}^{n-1} f(i)\}$ gives the desired bijection for infinite X.

What about supersets of $\mathbb{N}$? After Excercise 1 it shouldn't be hard for you to prove that adding a finite number of elements will not change the cardinality, but what if we double the number of elements ? Prove or disprove:

Excercise 1.4
$|\mathbb{N}| = |\mathbb{Z}|$.

The result of Excercise 1.4 can be generalized. Prove the following propositions:

Theorem 1.5
The union of two countable sets is countable.

Hint: Use the same technique as for Excercise 1.4; note to Excercise 1 might be helpful. Consider finite and infinte cases separately.

Theorem 1.6
Any subset of a countable set is countable.

Theorem 1.7
Intersection two countable sets is countable.

Theorem 1.8
Set difference two countable sets is countable.

Hint: Use Theorem 1.6

Now we can prove some intersting properties of infinite sets in general:

Theorem 1.9
Every infinite set has a countably infinite subset.

Hint: For a set X, look at the set Φ all injective maps from $\mathbb{N}$ into X. If Φ is empty, then all the maps from $\mathbb{N}$ to X are onto, and $|\mathbb{N}| \geq |X|$. You should be able to continue the proof from here.

Bonus Theorem 1.10 (Dedekind's Theorem)
A set is infinite if and only if there is a one-to-one function from the set into a proper subset of itself.

Hint: If X be infinite and has a countable subset Y, let $f(x) = x \forall x \notin Y$. Complete the definition of f so that f is a bijection between X and its proper subset. Write the proof in the other direction to complete the proof of the theorem.

Now we can move on to analyzing the first most interesting superset of $\mathbb{N}$, namely, $\mathbb{Q}$. This set has a lot of properties that make it substantially different from $\mathbb{N}$. For instance, there is a rational number between any two rational numbers. Indeed, let $a, c \in \mathbb{Q}$, then $b = \frac{a+c}{2} \in \mathbb{Q}$ and $a \leq b \leq c$. Also, any real number can be approximated with a rational number to an arbitrary degree: for intstance, $3.1415 = \frac{31415}{10000}$ is a rational apporximation of π to within 10^{-4}, but if we wanted a better one, we could just continue writing out the digits of π and get more and more precise approximations like 3.141592. This cannot be done with integers, which are a subset of $\mathbb{Q}$. Now one might think that $|\mathbb{Q}| > |\mathbb{N}|$ and, surprisingly, be wrong, as we shall demonstrate in what follows.

Theorem 1.11
$|\mathbb{N}| \leq |\mathbb{Q}| \leq |\mathbb{N} \times \mathbb{N}|$

Hint: recall that $|A| \leq |B|$ iff there is $\phi : A \Rightarrow B$ which is injective, and $|A| \geq |B|$ if there is $\phi : A \Rightarrow B$ surjective. Recall what it means for a number x to be rational.

Theorem 1.12
Union of countably many countable sets is of the same cardinality as $\mathbb{N} \times \mathbb{N}$

Hint: lay out the sets in the union on a lattice grid, $\mathbb{N} \times \mathbb{N}$.

Theorem 1.13, an important one
$\mathbb{N} \times \mathbb{N}$ is countable

Hint: look at the lattice grid. Start at the origin and try walking the grid in such a way that any point in it will be reached after a finite number of steps. One example of such walk would be drawing $\mathbb{Z} \times \mathbb{Z}$ and walking it in a spiral starting from the origin (see Figure 1); try to come up with other kinds of walks. Then the walk will be an enumeration of the points in $\mathbb{N} \times \mathbb{N}$, since it yields a bijection $\phi(n) =$(the point you reach after n steps)

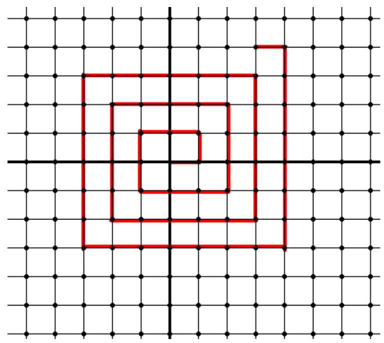

Figure 1: Lattice Walk on $\mathbb{Z} \times \mathbb{Z}$

Corollary 1.14
$\mathbb{Q}$ is countable.

Corollary 1.14
Union of countably many countable sets is countable.

Corollary 1.14
$\mathbb{N}^n = \underbrace{\mathbb{N} \times \mathbb{N} \times ... \times \mathbb{N}}_{n \text{ times}}$ is countable.

Now that we have seen that $\mathbb{Q}$ is countable, the question to solve would be whether $\mathbb{R}$ is countable or not. We shall approach this question slowly, first going back to subsets of $\mathbb{N}$ and seeing how they realate to $\mathbb{R}$.

Theorem 1.15
The set of all finite subsets of a countable set is countable.

Hint: make a list of such subsets; look at how many subsets there are of a certain fixed size.

Theorem 1.16
For any set A, there is a one-one function f from A into $P(A)$.

Theorem 1.17 (Cantor)
There is no function from a set A onto $P(A)$.

Hint: look at some function $\phi : A \Rightarrow P(A)$. Now for $a \in A$, $\phi(a) \subseteq A$ (why?). So for each element of A we have two cases:

1. $a \in \phi(a)$. Call such elements blue.
2. $a \notin \phi(a)$. Call such elements red.

Look at the set of all red elements to obtain a contradiction.

Cantors Theorem implies that $P(\mathbb{N})$ is not a countable set. A set that is not countable is called uncountable. So $P(\mathbb{N})$ is an uncountable set. In fact, Cantors theorem implies that there are infinitely many different infinite cardinal numbers:

Corollary 1.17
There are infinitely many different infinite cardinalities.
Now we know that there's an infinity of an order higher than that of the natural numbers. Is $\mathbb{R}$ a set whose order is of that kind ? Is $\mathbb{R}$ related to $P(\mathbb{N})$? We shall answer these questions in the following theorems.

Theorem 1.18
For a set A, let P be the set of all functions from A to the two point set $0, 1$. Then $|P| = |P(A)|$.

Hint: Each element in $P(A)$ can be looked at as a function that tells whether an element of A is in the subset or not.

Theorem 1.19
Show that if A is finite, then $|P(A)| = 2^{|}A|$

Hint: : use Theorem 1.18 to count all elements of $P(A)$.

Corollary 1.20
There is a one-one correspondence between $P(\mathbb{N})$ and infinite sequences of 0s and 1s.

Theorem 1.21
Let $I = |[0, 1)|$. Then $|I| = |P(\mathbb{N})|$.

Hint: write each number as infinite decimal.

Theorem 1.22
$|\mathbb{R}| = |[0, 1)|$

Hint: you need to find a bijection between $\mathbb{R}$ and $[0, 1)$. Perhaps the simplest one can be represented geometrically (see Figure 2)

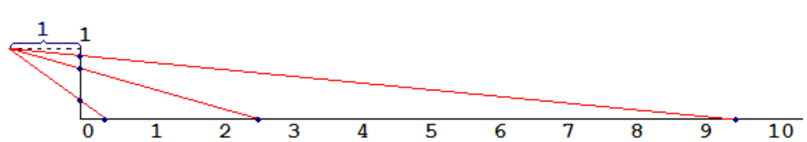

Figure 2: Each point on the vertical segment corresponds to a point on a line

Even though such demonstration by picture would be enough in most cases, you should understand the algebra behind it. Can you figure out the algebraic function $f : [0, 1) \Rightarrow \mathbb{R}$ represented on the picture ? You can come up with your own bijection.

Now the time has come to combine the results of the theorems we've proven.
Theorem 1.23

$|\mathbb{R}| = |P(\mathbb{N})| > |\mathbb{N}|$

At last, we've seen that there are more real numbers than natural numbers. To be more specific, we introduce the following notation: for a set A, 2^A denotes $P(A)$; $|\mathbb{N}| = \aleph_0$ (read: *aleph null*, from the name of the hebrew letter *aleph*), $2^{\aleph_0} = \aleph_1$, and in general $\aleph_{n+1} = 2^{\aleph_n}$. Then $|\mathbb{R}| = c = \aleph_1$. Now one might wonder whether $\aleph_0, \aleph_1, ...$ represent all possible cardinalities of infinte sets. In fact, all the common sets of numbers we use: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are either $\aleph_0$ or $\aleph_1$. Is there a set with cardinality between $\aleph_0$ and $\aleph_1$? Can we have a set with cardinality $\aleph_{0.7}$ or $\aleph_{1.5}$?

This question has bothered the minds of mathematicians for many years, and the proposition that there is *no* set with cardinality between $\aleph_0$ and $\aleph_1$ is known as the *Continuum Hypothesis*, conceived by Georg Cantor (he was also the one who proved all the theorems above and invented the $\aleph_n$ notation). Now how would one prove or disprove the hypothesis ? The answer is not simple. Here's an excerpt from Wikipedia: "Cantor believed the continuum hypothesis to be true and tried for many years to prove it, in vain. It

became the first on David Hilbert's list of important open questions that was presented at the International Mathematical Congress in the year 1900 in Paris.

Kurt Godel showed in 1940 that the continuum hypothesis (CH for short) cannot be disproved from the standard Zermelo-Fraenkel set theory, even if the axiom of choice is adopted. Paul Cohen showed in 1963 that CH cannot be proven from those same axioms either. Hence, CH is independent of ZFC. Both of these results assume that the Zermelo-Fraenkel axioms themselves do not contain a contradiction; this assumption is widely believed to be true."

So we can either safely assume existence or nonexistence of sets with cardinalities between $aleph_0$ and $aleph_1$ without ruining the basis on which current mathematics stands on. You are free to make your choice on the truth of the hypothesis.

Thus we finish our list of theorems to prove and turn to some problems.

<u>Problem 2.1</u>
Bob and joe are playing the following game: Joe secretly writes down a sentence, and Bob tries to read Joe's mind by telling precisely what Joe has written. Joe is a kind person, so he allows Bob to make infinite number of mistakes, and the sentence stays the same after each try. If Bob get the sentence correctly, Bob wins. Is there an optimal strategy for Bob ? Is there an optimal strategy for Joe ?

<u>Problem 2.2</u>
Bob and Joe are playing another game. Bob thinks of a real number, and Joe tries to guess it. Bob remembers how kind Joe was, and allows for infinite number of mistakes. An eternity passes, but Joe still can't get the number (why?), so Bob allows Joe to win even if he doesn't get the answer precisely. Now Joe has to guess the number to within $\frac{1}{10^{10000000000000000000000000000000}}$. Can Joe win now ? What if Bob thought of a point in $\mathbb{R}^n$ and made Joe guess the location to that precision ?

<u>Problem 2.3</u>
Suppose a submarine is moving in a straight line at a constant speed in the plane such that at each hour, the submarine is at a lattice point. Suppose at each hour you can explode one depth charge at a lattice point that will kill the submarine if it is there. You do not know where the submarine is nor do you know where or when it started. Prove that you can explode depth charges in such a way that you will be guaranteed to eventually kill the submarine.

<u>Geometrical Proof:</u>
Let X be the set of points of a unit hemisphere, i.e $X = \{(x, y, z) | x^2 + y^2 + z^2 = 1 \wedge z < 0\}$. Show that $|X| = |\mathbb{R}^2|$.

Hint: raise the hemishpere 1 unit up, so it lies on the cartesian plane; then the bijection is very similar the one in Figure 2. If the proof seems hard, try showing a bijection between the real number line and the set of points belonging to a unit semicircle $Y = \{(x, y) | x^2 + (y-1)^2 = 1 \wedge y < 1\}$

Interesting Fact

Let $X = [0, 1]$.Show that $|X| = |X^2|$. Then show that $|\mathbb{R}| = |\mathbb{R}^2|$. Then show that $|\mathbb{R}| = |\mathbb{R}^n|$ for any $n \in \mathbb{N}$.

Hint: each element in $[0, 1]$ can be written as a string $0.a_1a_2a_3...$, where $a_i \in \{0, 1, ..., 9\}$ are decimal digits. Any element of $[0, 1] \times [0, 1]$ can be written as a pair of such strings. Find a bijection between the set of strings and the set of pairs of strings.

Interesting Corollary

$|\mathbb{R}^n| = |[0, 1)|, \forall n \in \mathbb{N}$

Fun Bonus Problem on Function Composition

Prove that using only one operation $a * b = 1 - \frac{a}{b}$, one can get the sum, the product, the difference and the ratio of any two numbers. You may use ***only*** the two numbers a, b that are given and the operation $*$, i.e. to use a number or an operation, you have to express it first in terms of a, b and $*$.

So this is the end. Hopefully, you have enjoyed your homework !