Notes 11

Review sessions Monday 5-7 and 7-9 in room 3-270

Quiz one is 7-9 in rooms 3-270 and 3-370

Quiz covers material up through functions.

1 Infinite Sets

Last time we began to see that some of the intuitive results we'd expect from the pigeonhole principle break down when we deal with infinite sets. For example, if A and B are *finite* sets, and we know that B is a proper subset of A, then the following is true. For any function $f : A \to B$, there are two distinct elements of A that get mapped to the same element in B. This is just another way of looking at the pigeonhole principle.

But this "obvious" fact isn't even true for infinite sets. For example, A could be the natural numbers $\{0, 1, 2, \ldots\}$, B could be the even natural numbers $\{0, 2, 4, \ldots\}$, and the function $f(x) = 2x$ maps distinct elements of A to distinct elements of B.

So it's clear that infinite sets are pretty tricky things, and we need to be careful in how we handle them. Let's start with a formal definition of what it means for a set to be infinite.

Definition 1.1 We say that a set S is finite if there is an $n \in \mathbb{N}$ and a bijection $f : [n] \to S$.

Definition 1.2 We say that a set T is infinite if it is not finite. That is, T is infinite if for every $n \in \mathbb{N}$, T has more than n elements.

So for example, the set $\{1, 2, \ldots, n\}$ is finite for each n, but $\mathbb{N}$ is infinite.

As a more interesting proof that a set is infinite, consider the following.

Theorem 1.3 The set P of all prime numbers is infinite.

Proof. By contradiction. Suppose that P is finite; then there is an $n \in \mathbb{N}$ so that $P = \{p_1, \ldots, p_n\}$. By the fundamental theorem of arithmetic, this would mean that every natural number would have a factor from this finite set. In particular, the number $m = p_1 p_2 \cdots p_n + 1$

would have such a factor. That is, for some i, $p_i \mid m$. But we also have $m - 1 = p_1 p_2 \cdots p_n$, so $p_i \mid m - 1$. Since $p_i \mid m$ and $p_i \mid m - 1$, we have $p_i \mid 1$, a contradiction. ∎

It's not always so easy to show that a set of natural numbers is infinite. For example, the following is a famous open problem in number theory.

Definition 1.4 A *twin prime* is a pair $(n, n+2)$ where both n and $n+2$ are prime.

So $(3, 5)$, $(11, 13)$, and $(101, 103)$ are all examples of twin primes.

Question: Are there an infinite number of twin primes?

This question goes back to the ancient Greeks, and we still don't know the answer.

2 Countability

As we've seen, if we have a finite set S, we can write it as $S = \{s_1, \ldots, s_n\}$ for some natural number n. There are some infinite where a related kind of "listability" property holds — that is, there are infinite sets T for which we can list out the elements in such a way that for every $t \in T$, there is a natural number i so that t eventually appears as the i^{th} element of the list.

Let's show some examples of what we mean:

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

$$\text{evens} = \{0, 2, 4, 6, \ldots\}$$

$$\text{primes} = \{2, 3, 5, 7, \ldots\}$$

In the first case, the natural number n will appear as the n^{th} entry in the list. (If we number the entries starting from 0.) In the second case, the even number $2k$ will appear as the k^{th} entry in the list. In the third case, we can argue that every prime number will eventually appear as an entry in the list, though we don't have a nice closed form expression for which entry a given prime number p will appear as.

The infinite sets that can be listed in this way are said to be *countable sets*. They are called countable because one can count their items one after the other so that every item is eventually counted. Formally, we are saying that they can be put in a one-to-one correspondence with the natural numbers (this represents the way in which we "count" them).

Definition 2.1 An infinite set T is said to be *countably infinite* iff there is a bijection $f : \mathbb{N} \to T$.

Definition 2.2 A set S is said to be *countable* if it is finite or is countably infinite.

So for example, the even numbers are countably infinite because $f : \mathbb{N} \to$ evens defined by $f(i) = 2i$ is a bijection between the naturals and the even numbers.

In fact, to prove countability it is sufficient to prove that there is a *surjection* from $\mathbb{N}$ to S. It can be proved that in this case, either S is finite, or there is also an injection from $\mathbb{N}$ into S.

3 Uncountability

When you first see the notion of countably infinite sets, there is no compelling reason not to think (as Georg Cantor did in the 1870's when he introduced the idea of countability) that all infinite sets are countable. But this is in fact not true, and the real numbers provide a counterexample. After failing to put the set $\mathbb{R}$ of all real numbers in a bijection with the naturals, Cantor came up with the following remarkable proof that in fact there cannot exist such a bijection.

Theorem 3.1 $\mathbb{R}$ is not countable.

Proof. For simplicity, we will show that there exists no bijection from $\mathbb{N}$ to the unit interval $[0, 1] \subset \mathbb{R}$.

The proof is by contradiction; suppose that $f : \mathbb{N} \to [0, 1]$ is a bijection.

Now there's some notational trouble in deciding how to represent a real number in the unit interval — let's represent it in decimal expansion; and for those real numbers that have terminating decimal expansions, we'll add on an infinite string of 0's at the end. (So, for example, .23 will be written as $.2300000\cdots$.) Some real numbers have non-unique representation (for example $.19999\cdots = .20000\cdots$) so we will adopt the convention of keeping only the representation that terminates in a string of 0's.

The proof will use a method called *diagonalization*; roughly, it goes as follows. We construct a number r and show

(i) It is a valid real number.

(ii) It is not equal to $f(i)$ for any natural number i.

This will give a contradiction to our assumption that f is a bijection.

We construct r digit by digit. To get the i^{th} digit of r, we take the i^{th} digit of $f(i)$ and add 5 to it modulo 10. We can picture this construction using the following table.

$$\begin{array}{cccccccc}
f(0) & = & . & \mathbf{3} & 1 & 4 & 3 & \cdots \\
f(1) & = & . & 5 & \mathbf{8} & 2 & 9 & \cdots \\
f(2) & = & . & 9 & 1 & \mathbf{1} & 1 & \cdots \\
f(3) & = & \cdots & \cdots & \cdots & \cdots & \mathbf{2} & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots
\end{array}$$

Then, following our recipe for constructing r, it would begin $r = .8367\cdots$. The term "diagonalization" comes from the fact that we're moving down the (boldface) diagonal of this infinite table, explicitly changing digits as we go.

Now let's observe that $r \in [0, 1]$, since we have specified its decimal expansion.

But (the crucial point), we claim that r is not equal to $f(i)$ for any natural number i. To see this, suppose that $r = f(j)$. But r differs from $f(j)$ by 5 in the j^{th} decimal place; this would contradict the fact that $r = f(j)$. (One might worry that there is more than one representation for a real number, e.g. $.9999\ldots = 1$, but it is easy to verify that such representation can differ by at most 1 in any decimal place, so there is no way for r to be present in the table under some other guise).

Thus, f does not map any natural number to r; this contradicts our assumption that f was a bijection. ∎

Diagonalization arguments (of which this was the first, historically) have become very important in logic and computer science. In 6.045, you'll use them to show that there are some problems that cannot be solved by any computer program.

4 Proving Sets are Countable

The usual way to prove a set is countable is to construct an explicit "listing" of it — that is, an explicit bijection with the naturals. Let's try this out on a few sets.

Theorem 4.1 The integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ are countable.

Proof. We list the integers as $0, -1, 1, -2, 2, -3, 3, \ldots$. To decide if this is a valid listing (i.e. a bijection with the naturals), we need to consider the following question:

(*) For every integer x, is there a natural number i so that x will appear as the i^{th} element of the list?

In this case, the answer is yes — if $x = 0$ then $i = 0$; if $x < 0$ then $i = 2x - 1$; and if $x > 0$ then $i = 2x$.

Note that there are some listings of $\mathbb{Z}$ that are of no use in proving it is countable. For example, consider

$$\mathbb{Z} = 0, 1, 2, 3, \ldots, -1, -2, -3, \ldots.$$

We ask the same question (*) — but now, there is no natural number i so that -1 appears as the i^{th} entry of the list. ■

How about the set of half integers? It is also countable since we can establish a bijection with $\mathbb{N}$ by $\{0, 1/2, -1/2, 1, -1, \ldots\}$.

Theorem 4.2 If A and B are countable sets, so is $A \cup B$.

Proof.

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

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

$$A \cup B = \{a_1, b_1, a_2, b_2, \ldots\}$$

■

Now let's consider a set that seems much bigger than the natural numbers — $\mathbb{Q}$, the set of rational numbers. Actually, to keep our notational headaches to a minimum, let's talk about $\mathbb{Q}^+$, the set of positive rational numbers. (The arguments are roughly the same in either case.)

So is $\mathbb{Q}^+$ countable or uncountable? There are certainly some problems with counting it – since there is no smallest positive rational, it's not clear where to begin; and between any two positive rationals there is another positive rational. Nevertheless, $\mathbb{Q}^+$ is a countable set, and the proof of this introduces a very useful "dove-tailing" technique for counting a set. This proof actually introduces a *surjection* from $\mathbb{N}$ to $\mathbb{Q}^+$, but as we've mentioned before, this is sufficient to guarantee a bijection as well.

Theorem 4.3 The set $\mathbb{Q}^+$ is countable.

Proof. The positive rational numbers are precisely those numbers that can be written in the form a/b, where a and b are positive natural numbers. To make sure that we eventually get to all the elements of $\mathbb{Q}^+$, we list them in the following order:

(1) All a/b with $a + b = 2$,

(2) All a/b with $a + b = 3$,

(3) All a/b with $a + b = 4$,

... and so on ...

The point here is that for any k, there are at most $k+1$ rational numbers of the form a/b, where $a+b=k$ — so in each of the above steps, we only have to list a finite number of rationals.

We can picture this way of listing the rationals using the following table:

$$\begin{array}{ccccc} 1/1 & 2/1 & 3/1 & 4/1 & \cdots \\ 1/2 & 2/2 & 3/2 & 4/2 & \cdots \\ 1/3 & 2/3 & 3/3 & 4/3 & \cdots \\ 1/4 & 2/4 & 3/4 & 4/4 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{array}$$

We sweep diagonally through this table, listing the numbers as

$$1/1, 2/1, 1/2, 3/1, 2/2, 1/3, 4/1, \ldots$$

Note that a number like 1 will get listed many times — as $1/1, 2/2, 3/3, \ldots$. But this is not a problem, since we can just remove it from the list every time it appears after the first.

As always, to see if this is a valid listing, we have to ask the following question:

(*) For every positive rational a/b, is there a natural number i so that x will appear as the i^{th} element of the list?

Again, the answer is yes. a/b will be listed by the time we reach step $a+b$ — that is, it will be entry i for some i that is at most $(a+b+1)^2$. ■

What about the negative rationals? Clearly they are also countable since we can replace q with $-q$ in the list of the previous theorem. Then from the theorem we proved earlier we conclude that $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^-$ is also countable.

This method of listing (called "dove-tailing") can be used to show that the cross product of countable sets is countable.

Theorem 4.4 If A and B are countable sets, so is $A \times B$.

Proof. Let $A = \{a_1, a_2, \ldots\}$, $B = \{b_1, b_2, \ldots\}$, and list them

$$\begin{array}{cccc} (a_1, b_1) & (a_1, b_2) & (a_1, b_3) & \cdots \\ (a_2, b_1) & (a_2, b_2) & (a_2, b_3) & \cdots \\ (a_3, b_1) & (a_3, b_2) & (a_3, b_3) & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{array}$$

Now we can count them using dove-tailing. ■

A "dovetail" in carpentry is a fan-shaped piece of wood that interlocks with other fan-shaped parts of a "mortise", interleaving the two components into one. Here we are fitting infinite sequences together instead. Going further back, I think the carpentry term refers to the smooth interlocking in the feathers of a dove's tail.

Now let S_n be the set of the n-digit decimals, and let $S = \bigcup_{i=1}^{\infty} S_n$. Is S countable?

First, let's show that it's uncountable

Proof. By contradiction. Assume S is countable and list it's elements. $S = \{s_1, s_2, \ldots\}$.

Define the number $x = .x_1 x_2 \ldots$ by letting $x_i = s_i + 5(\mod 10)$. Then x is not S, and we obtain the desired contradiction. ■

Now let's prove it's countable.

Proof. Just list S_1 (which is finite), then list S_2 and so on. So S is countable. ■

What's wrong here? Well, S is the set of all decimal numbers with *finite* decimal expansions. x in the first proof is an number with an infinite expansion, so the fact that it's not in S is not a contradiction.

5 Sizes of Infinite Sets

We said earlier, without really thinking too hard about it, that two finite sets have the same size if they have the same number of elements. But when we get to infinite sets, it becomes tricky to define what it means for two sets to be "the same size".

The best way to define this seems to be in terms of bijections. We say that A and B have the same size, written $|A| = |B|$, if there is a bijection from A to B.

So for example, $|\mathbb{N}| = |\mathbb{Q}|$, but $|\mathbb{N}| \neq |\mathbb{R}|$. More generally, we say

Definition 5.1 $|A| \leq |B|$ iff there is an injection $f : A \to B$.

Definition 5.2 $|A| \geq |B|$ iff there is a surjection $f : A \to B$.

Definition 5.3 $|A| = |B|$ iff there is a bijection $f : A \to B$.

We extend these definitions in obvious ways, e.g. $|A| < |B|$ means $|A| \leq |B|$ but $|A| \neq |B|$—that is, there is an injection from A to B but no bijection. These definitions are actually consistent the way we'd like them to be. One can prove (though it is harder than one might think) that $|A| \leq |B|$ imples $|B| \geq |A|$, that $|A| \leq |B|$ and $|B| \leq |A|$ implies $|A| = |B|$, and so on. Such statements are not at all obvious from the definitions, but we'll just take them as given.

After showing that $|\mathbb{N}| < |\mathbb{R}|$, Cantor asked the next most natural question: is there an infinite sequence of infinite sets $A_0, A_1, A_2, \ldots$, so that for each i we have $|A_i| < |A_{i+1}|$? That is, are there infinitely different "types" of infinite sets, none of which can be put in bijection with each other.

Cantor showed that the answer to this question is yes, with the following sweeping generalization of $|\mathbb{N}| < |\mathbb{R}|$. Recall that if S is a set, we use $\mathcal{P}(S)$ to denote the *power set* of S — that is, the set of all subsets of S.

Theorem 5.4 For all sets S, we have $|S| < |\mathcal{P}(S)|$.

Proof. We have to show two things: $|S| \leq |\mathcal{P}(S)|$, and $|S| \neq |\mathcal{P}(S)|$.

To show the first, we need to find an injection $g : S \to \mathcal{P}(S)$. This is not so difficult; we could define g by $g(a) = \{a\}$ for each $a \in S$.

To show the second fact (the hard part), we need to show there is not bijection $f : S \to \mathcal{P}(S)$. This is tricky because we cannot list S.

Suppose there were such a bijection f; we want to get a contradiction. The argument that gives the contradiction is actually very short, but very tricky; it is based on the idea behind Russell's Paradox.

For $a \in S$, $f(a)$ is a subset of S, so it makes sense to ask whether or not a is an element of $f(a)$. Let's define $T \subset S$ as

$$T = \{a \in S \mid a \notin f(a)\}.$$

Now, since we're supposing f is a bijection, there is some $b \in S$ such that $f(b) = T$.

Now we ask: is b an element of T?

- Case 1: $b \in T$. Then since $T = f(b)$, we have $b \in f(b)$, contradicting the definition of T.
- Case 2: $b \notin T$. Again, since $T = f(b)$, we have $b \notin f(b)$, contradicting the definition of T.

As we get a contradiction in either case, our assumption that f is a bijection must be wrong. ∎

So this answers the question about an infinite "increasing sequence" of infinite sets. We can take

$$\begin{array}{rcl} A_0 & = & \mathbb{N} \\ A_1 & = & \mathcal{P}(\mathbb{N}) \\ A_2 & = & \mathcal{P}(\mathcal{P}(\mathbb{N})) \\ \dots & \dots & \dots \\ A_{i+1} & = & \mathcal{P}(A_i) \\ \dots & \dots & \dots \end{array}$$

This list produces some *really* big sets. We can show that $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$ by giving a bijection between them (we won't do this here) — so we could just as well have used $\mathbb{R}$ as the set A_1.

The quantity $|A|$, for a set A, is called a *cardinality*, and we can use a variable to denote it. Usually we write $\aleph_0$ for $|\mathbb{N}|$, $\aleph_1$ for the next largest cardinality of infinite set, and so on.

Does this list use up all possible cardinalities? No, we can define a new set $A = \cup_{n=0}^{\infty} \aleph_n$. This set clearly contains (and is thus at least as large as) every possible $\aleph_n$. Therefore, $\mathcal{P}(A)$ is strictly larger than every $\aleph_n$. In fact, it is easy to modify this argument to prove that there is no largest set.

Cantor asked one more very natural question. Namely, does our list of increasing sets $A_0, A_1, \dots$ "skip" any of the possible cardinalities of sets? That is, could there be an infinite set B so that for some A_i on the list, $|A_i| < |B| < |A_{i+1}|$? The conjecture that there is no such "in-between" set B is the *Generalized Continuum Hypothesis*; the weaker conjecture, that at least there is no B in between $\mathbb{N}$ and $\mathbb{R}$, is the *Continuum Hypothesis.*

Cantor didn't see how to settle the Continuum Hypothesis, and at the International Congress of Mathematicians in 1900, this was the first problem on David Hilbert's list of 24 open problems for the coming century. The question was finally resolved by Paul Cohen in 1963, in a very strange way. He didn't construct a set B so that $|\mathbb{N}| < |B| < |\mathbb{R}|$, and he didn't prove that such a set can't exist. Instead, he showed that the existence of such a set was independent of the axioms of set theory. That is, provided the axioms of set theory are consistent, you could include a new axiom asserting the existence of such a B, or you could include a new axiom asserting that no such B exists — and either way, the axioms would remain consistent. This "independence" result came as a big surprise, and it's certainly one of the nicest theorems of 20th century mathematics.