COMPSCI 230: Discrete Mathematics for Computer Science March 27, 2019

Lecture 19

Lecturer: Debmalya Panigrahi *Scribe: Kevin Sun*

1 Overview

In this lecture, we will learn how to compare the "sizes" of two sets that both have an infinite number of elements. We will also formalize our intuition that some infinite sets are "larger" than others.

2 Comparing Sizes via Functions

In the late nineteenth century, the mathematician Georg Cantor began pioneering the study of the "size" of infinite sets. He realized that intuitively, some infinite sets are "larger" than others (e.g., $\mathbb{R}$ is "larger" than $\mathbb{Z}$), but at the time, the formalization of this distinction was lacking. Therefore, he devised the idea of using *functions* to capture the different "kinds" of infinite sets.

Let A and B be two (possibly infinite) sets. Recall that we say A surj B if there exists a surjective function from A to B. Intuitively, this means that the size of A is at least as large as the size of B, because a surjective function must use the elements of A to "hit" every element of B, and each element of A can only get mapped to one element of B.

Indeed, if A and B are finite sets, then A surj B if and only if $|A| \geq |B|$ (see Lecture 8). However, if A and B are infinite sets, the cardinalities $|A|$ and $|B|$ are no longer defined but "A surj B" is still well-defined. With this in mind, we will re-examine a few basic properties concerning the cardinality of sets. Recall that A bij B means there exists a bijective function from A to B, and A inj B means there exists a (total) injective function from A to B.

Theorem 1. *Let A, B, C be (possibly infinite) sets. Then the following propositions are all true:*

1. *A surj B and B surj C implies A surj C.*
2. *A bij B and B bij C implies A bij C.*
3. *A bij B implies B bij A.*
4. *A surj B if and only if B inj A.*
5. *A surj B or B surj A.*
6. *(Schröder-Bernstein Theorem.) A inj B and B inj A implies A bij B.*

Proof. The proofs of properties 1-3 are similar to those for finite sets, but for completeness, we include these proofs for infinite sets below. The proofs of the last 3 properties for infinite sets are beyond the scope of this class, and are hence omitted. We will prove each property individually—for finite sets, many of these statements were proven using cardinality rules in Lecture 8.

1. Let $f : A \to B$ and $g : B \to C$ be surjections. We claim that the function $h : A \to C$ defined by $h(x) = g(f(x))$ is also a surjection. Let c be an arbitrary element of C. Since g is surjective, there exists $b \in B$ such that $g(b) = c$. Since f is surjective, there exists $a \in A$ such that $f(a) = b$. Thus, $h(a) = g(f(a)) = g(b) = c$.

2. Let $f : A \to B$ and $g : B \to C$ be bijections. We claim that the function $h : A \to C$ defined by $h(x) = g(f(x))$ is also a bijection. From proposition (1) above, we know that h is surjective. Furthermore, let a_1 and a_2 be distinct elements of A. Since f is injective, we know $f(a_1) \neq f(a_2)$. Since g is injective, we know $g(f(a_1)) \neq g(f(a_2))$. This last statement is precisely $h(a_1) \neq h(a_2)$, as desired.

3. If $f : A \to B$ is a bijection, then for each $b \in B$, there exists one element $a \in A$ such that $f(a) = b$. Let $f^{-1}(b)$ denote this single element of A. Now we can see that the function $g : B \to A$ defined by $g(y) = f^{-1}(y)$ is a bijection. □

Again, all of the propositions listed in Theorem 1 are true in both the finite and infinite cases. The proofs for the finite case are fairly straightforward, but become much less so in the infinite case. Now we will see a statement about the size of a set that only applies when the set is infinite.

Theorem 2. *Let A be a set, and let b be any element not in A. Then A is infinite if and only if there exists a bijection from $A \cup \{b\}$ to A.*

Before beginning the proof, we note that if A is finite and $b \notin A$, then $|A \cup \{b\}| = |A| + 1 > |A|$, so there clearly cannot be a bijection from $A \cup \{b\}$ to A. (In fact, there does not even exist an injection from $A \cup \{b\}$ to A.) However, the theorem states that if A is infinite, then such a bijection does exist. This is fairly counter-intuitive, because the existence of bijection informally means that $A \cup \{b\}$ and A have the "same size," even though the latter is a strict subset of the former.

Proof. The above discussion proves one direction of the theorem: if A is finite, then $|A \cup \{b\}| > |A|$, so there does not exist a bijection from $A \cup \{b\}$ to A.

Now suppose A is infinite—we must construct a function $f : A \cup \{b\} \to A$ that is a bijection. The most natural first attempt is the following: for all $x \in A$, set $f(x) = x$. However, this leaves no "room" in the codomain A for the element b. Thus, our strategy is the following: we will order an infinite subset of A in an (infinite) sequence, and shift every element "right" by 1. Then every element still has a spot, and the first spot is now free for b.

We now begin the formal proof. Since A is infinite, there exists some element of A which we denote by a_1. Furthermore, there also exists some element of $A \setminus \{a_1\}$, which we denote by a_2. In fact, this process can continue for every positive integer n: at step n, we can always find an element $a_n \in A \setminus \{a_1, \ldots, a_{n-1}\}$: simply pick n elements in A and discard elements in $\{a_1, \ldots, a_{n-1}\}$ if you picked them.

Let $S = (a_1, a_2, \ldots)$ be the infinite sequence of elements of A generated by the procedure described above. Note that S may not necessarily contain every element of A: for example, if $A = \mathbb{Z}^+$, then it is possible for the procedure above to return the sequence $S = (1, 3, 5, \ldots)$. (Indeed, we will see later that there are infinite sets A where S *necessarily* does not contain all elements of A!)

We now partition $A \cup \{b\}$ according to S, and define a function f as follows:

- If $x = b$, then set $f(x) = a_1$.
- If $x \in A \setminus S$, then set $f(x) = x$.

- If $x \in S$, then $x = a_k$ for some positive integer k. In this case, set $f(x) = a_{k+1}$.

It is not too difficult to see that $f : A \cup \{b\} \to A$ is bijective. The function f maps each element of $S \cup \{b\}$ to exactly one element of S, and every element of S is in the range of f. Also, f maps each element of $A \setminus S$ to itself, so overall, f is both surjective and injective. □

Remark: The proof above is closely related to a thought experiment known as Hilbert's paradox of the Grand Hotel. We can think of S as an infinite sequence of existing hotel guests, and every room is occupied. The element b checks in, and the hotel—despite being full—can accommodate for b by shifting every guest one room to the "right." This makes "room" for b to enter the hotel, and at the same time, each of the previous guests still has a place to stay. This paradox illustrates the counterintuitive nature of infinite sets and serves a reminder to avoid making assumptions without proof about infinite sets, even if they seem correct at first glance.

2.1 Countably Infinite Sets

We now begin studying one particular class of infinite sets, known as *countably infinite* sets. Intuitively, an infinite set A is countably infinite if it has the same "size" as the set of positive integers $\mathbb{Z}^+$. This means we can "count" the elements of A, one by one, in a way such that every element of A is eventually counted.

Definition 1. *Let A be a set. Then A is* countably infinite *if A bij $\mathbb{Z}^+$. If A is countably infinite or finite, then we say A is* countable. *If A is not countable, then we say A is* uncountable.

Remark: In Theorem 1, we saw that A bij B implies B bij A. Thus, an equivalent definition of "countably infinite" is the following: a set A is countably infinite if there exists a bijection $f : \mathbb{Z}^+ \to A$. This perspective corresponds to the notion of "counting" the elements of A one by one: the element $f(n)$ can be viewed as the "n-th element of A" for every $n \in \mathbb{Z}^+$.

In Problem 3(d) of Recitation 5, we gave a bijection from $\mathbb{Z}$ to $\mathbb{Z}^+$, proving that $\mathbb{Z}$ is countably infinite. From the alternate perspective, we can "count" every element of $\mathbb{Z}^+$ by proceeding in the following order: $(0, -1, 1, -2, 2, \ldots)$. Can we similarly count the positive rationals? At first glance, this looks difficult: if our list starts with $(a, b, \ldots)$, then it seems that we have "missed" all of the (infinitely many) rationals between a and b. However, with some more care, we actually *can* count the rational numbers.

Theorem 3. *The set of positive rational numbers $\mathbb{Q}^+$ is countably infinite.*

Proof. Note that finding an *injection* from $\mathbb{Z}^+$ to $\mathbb{Q}^+$ is trivial, since $\mathbb{Z}^+$ is a subset of $\mathbb{Q}^+$. Thus, the difficulty of the problem is finding a function from $\mathbb{Z}^+$ that is both injective *and surjective*—somehow, we must be able to "count" every positive rational number without "missing" any.

Recall that every positive rational can be written as a/b where $a, b \in \mathbb{Z}^+$. Now we shall use the notation (a, b) to represent the rational number a/b. Thus, the elements of $\mathbb{Q}^+$ can be arranged in a matrix, as shown in Fig. 1. The first row of the matrix contains all rationals with numerator 1, and in general, the i-th row of the matrix contains all rationals with numerator i.

$$\begin{tikzcd}
(1,1) \arrow[r] & (1,2) \arrow[dl] & (1,3) \arrow[r] & (1,4) \arrow[dl] & \cdots \\
(2,1) \arrow[d] & (2,2) \arrow[ur] & (2,3) \arrow[dl] & (2,4) & \cdots \\
(3,1) \arrow[ur] & (3,2) \arrow[dl] & (3,3) \arrow[ur] & (3,4) \arrow[dl] & \cdots \\
(4,1) & (4,2) \arrow[ur] & (4,3) & \cdots & \\
\vdots & \vdots & \vdots & \vdots &
\end{tikzcd}$$

Figure 1: A visual representation of the dovetailing bijection from $\mathbb{Q}^+$ to $\mathbb{Z}^+$.

Now we proceed with an argument known as *dovetailing*. Recall that we are trying to find a bijection $f : \mathbb{Q}^+ \to \mathbb{Z}^+$, so for every positive rational (i, j), we must specify a positive integer $f((i, j))$. For notational convenience, we write $f(i, j)$ instead of $f((i, j))$. This specification is given by following the arrows shown in Fig. 1: $f(1, 1) = 1, f(1, 2) = 2, f(2, 1) = 3, f(3, 1) = 4, \ldots$

More formally, we can define f by partitioning the matrix in Fig 1 into diagonals, and each diagonal corresponds to a contiguous subset of $\mathbb{Z}^+$. The first diagonal is simply $\{(1, 1)\}$, and the corresponding subset of $\mathbb{Z}^+$ is $\{1\}$. In general, the elements of the k-th diagonal are exactly the (i, j) such that $i + j = k + 1$, and there are always exactly k such elements. Starting with $f(1, 1) = 1$, the function f maps the elements of the k-th diagonal to the smallest k elements of $\mathbb{Z}^+$ that aren't in the range of f applied to the previous $k - 1$ diagonals.

This function is clearly surjective: by dovetailing long enough, we will eventually reach any positive integer. However, as stated, it is not injective: for example, we have $f(1, 1) = 1 \neq 5 = f(2, 2)$ even though $(1, 1)$ and $(2, 2)$ represent the same element of $\mathbb{Q}^+$. To remedy this, we can simply "skip" any repeated elements of $\mathbb{Q}^+$ as we construct f in the dovetailing. In this case, we would set $f(3, 1) = 4$, skip $(2, 2)$ (because it has already been defined by $f(1, 1)$, and set $f(1, 3) = 5$. □

The dovetailing technique used in the proof of Theorem 3 also, in fact, proves a much more general theorem.

Theorem 4. *Let A_n be a countably infinite set for every $n \in \mathbb{Z}^+$. Then the set $A = \cup_{i=1}^{\infty} A_n$ is also countably infinite. In other words, the union of a countable number of countable sets is countable.*

Proof. The formal proof relies on the Axiom of Choice, which we shall not discuss. Although the following proof is informal, it provides an intuitive justification of Theorem 4. Recall that in the proof of Theorem 3, we counted the rationals as follows: at step t, we counted the smallest uncounted element in the first t rows of the matrix.

Now we can prove Theorem 4 by visualizing each set A_n as a row in a matrix. The same dovetailing process still works: at step t, we count the t-th element of A_1, the $(t-1)$-th element of A_2, and so on, until the first element of A_t. We then continue to step $t+1$. This counting procedure produces a bijection between A and $\mathbb{Z}^+$, as desired. □

Note that Theorem 3 is now a simple corollary of Theorem 4. In this case, we can think of A_n as all of the positive rationals with numerator n, and so $\mathbb{Q}^+$ is essentially $\cup_{n=1}^{\infty} A_n$. Since A_n is countably infinite for every $n \in \mathbb{Z}^+$, Theorem 4 tells us that $\mathbb{Q}^+$ is countably infinite.

2.2 Beyond Countable Sets

We now look at sets that are not countable. These sets are, in some sense, "even larger" than countably infinite; in other words, there is *no* way to arrange their elements in a list such that every element is eventually listed.

Recall that if A is a set, then 2^A represents the set whose elements are all subsets of A. If A is finite and has size $|A|$, then 2^A has exactly $2^{|A|}$ elements, so 2^A is much larger than A. This means there cannot be a bijection between A and 2^A. If A is infinite, then although the meaning of "$|A|$" is not clear, the conclusion remains the same.

Theorem 5. *Let A be a (possibly infinite) set. Then there is no bijection between A and 2^A.*

Proof. For contradiction, assume there exists $g : A \to 2^A$ such that g is a bijection. Thus, each input to g is an element of A, and each output of g is a subset of A. Consider the following set:

$$B = \{a \in A : a \notin g(a)\}.$$

It is clear that B is a subset of A, so $B \in 2^A$. Since g is bijective, there exists $a' \in A$ such that $g(a') = B$. Now let us consider the proposition P, which states "a' is an element of B."

- If P is true, then $a' \in B = g(a')$. But from the definition of B, this means $a' \notin B$. In other words, P is true implies P is false, so P cannot be true.
- However, if P is false, then $a' \notin B$, so $a' \notin g(a')$, which means $a' \in B$ from the definition of B. This means P is true, but we already know P cannot be true.

Thus, our assumption that a bijection $g : A \to 2^A$ exists has led us to a proposition that is neither true nor false. Since this is a contradiction, we conclude that there does not exist a bijection from A to 2^A.

Remark: The definition of B is closely related to Russell's paradox (see Lecture 1). This technique is known as *diagonalization*, which we shall see more of in our next lecture. □

As a corollary of Theorem 5, we can see that there exist sets that are not countably infinite. For example, setting $A = \mathbb{Z}^+$ gives us the following theorem.

Corollary 6. *The power set of $\mathbb{Z}^+$ is uncountable.*

Proof. Let $A = \mathbb{Z}^+$, so 2^A is clearly not finite. For contradiction, assume 2^A is countably infinite. This means there exists a bijection between 2^A and $\mathbb{Z}^+ = A$. But this contradicts Theorem 5, so 2^A is uncountable. □

3 Summary

In this lecture, we learned how to formally compare infinite sets in terms of their "size". We saw that one type of infinite sets is known as countably infinite, and there exist sets that are not countably infinite. Along the way, we saw a technique known as dovetailing, which allows us to systematically count the elements of a countably infinite set.