EE5110: Probability Foundations for Electrical Engineers **July-November 2015**

Lecture 3: Cardinality and Countability

Lecturer: Dr. Krishna Jagannathan *Scribe: Ravi Kiran Raman*

3.1 Functions

We recall the following definitions.

Definition 3.1 *A* **function** $f : A \rightarrow B$ *is a rule that maps every element of set* A *to a unique element in set* B*.*

In other words, $\forall x \in A, \exists y \in B$ and only one such element, such that, $f(x) = y$. Then y is called the image of x and x, the pre-image of y under f. The set A is called the domain of the function and B, the co-domain. $\mathcal{R} = \{y : \exists x \in A,\ s.t.\ f(x) = y\}$ is called as the range of the function f.

Definition 3.2 *A function* $f : A \rightarrow B$ *is said to be an* **injective (one-to-one) function***, if every element in the range* $\mathcal{R}$ *has a unique pre-image in* A*.*

Definition 3.3 *A function* $f : A \rightarrow B$ *is said to be a* **surjective (onto) function***, if* $\mathcal{R} = B$*, i.e,* $\forall y \in B,\ \exists x \in A,\ s.t.\ f(x) = y$*.*

Definition 3.4 *A function* $f : A \rightarrow B$ *is a* **bijective function** *if it is both injective and surjective.*

Hence, in a bijective mapping, every element in the co-domain has a pre-image and the pre-images are unique. Thus, we can define an inverse function, $f^{-1} : B \rightarrow A$, such that, $f^{-1}(y) = x$, if $f(x) = y$. In simple terms, bijective functions have well-defined inverse functions.

3.2 Cardinality and Countability

In informal terms, the cardinality of a set is the number of elements in that set. If one wishes to compare the cardinalities of two finite sets A and B, it can be done by simply counting the number of elements in each set, and declare either that they have equal cardinality, or that one of the sets has more elements than the other. However, when sets containing infinitely many elements are to be compared(for example, $\mathbb{N}$ versus $\mathbb{Q}$), this elementary approach is not efficient to do it. In the late nineteenth century, Georg Cantor introduced the idea of comparing the cardinality of sets based on the nature of functions that can be possibly defined from one set to another.

Definition 3.5 *(i) Two sets* A *and* B *are* **equicardinal** *(notation* $|A| = |B|$*) if there exists a bijective function from* A *to* B*.*

(ii) B *has cardinality greater than or equal to that of* A *(notation* $|B| \geq |A|$*) if there exists an injective function from* A *to* B*.*

(iii) B has cardinality strictly greater than that of A (notation $|B| > |A|$) if there is an injective function, but no bijective function, from A to B.

Having stated the definitions as above, the definition of countability of a set is as follow:

Definition 3.6 *A set E is said to be* **countably infinite** *if E and $\mathbb{N}$ are equicardinal. And, a set is said to be* **countable** *if it is either finite or countably infinite.*

The following are some examples of countable sets:
1. *The set of all integers $\mathbb{Z}$ is countably infinite.*
We can define the bijection $f : \mathbb{Z} \to \mathbb{N}$ as follows :

$n = f(z) \in \mathbb{N}$	$z \in \mathbb{Z}$
1	0
2	+1
3	-1
4	+2
5	-2
.	.
.	.
.	.

The existence of this bijective map from $\mathbb{Z}$ to $\mathbb{N}$ proves that $\mathbb{Z}$ is countably infinite.

2. *The set of all rationals in* $[0, 1]$ *is countable.*
Consider the rational number $\frac{p}{q}$ where $q \neq 0$. Increment q in steps of 1 starting with 1. For each such q and $0 \leq p \leq q$, add the rational number $\frac{p}{q}$ to the set, if it not already present. By this way, the set of rational numbers in $[0, 1]$ can be explicitly listed as: $\{0, 1, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \frac{1}{6}, \frac{5}{6}, ...\}$
Clearly, we can define a bijection from $\mathbb{Q} \cap [0, 1] \to \mathbb{N}$ where each rational number is mapped to its index in the above set. Thus the set of all rational numbers in $[0, 1]$ is countably infinite and thus countable.

3. *The set of all Rational numbers, $\mathbb{Q}$ is countable.*
In order to prove this, we state an important theorem, whose proof can be found in [1].

Theorem 3.7 *Let $\mathcal{I}$ be a countable index set, and let E_i be countable for each $i \in \mathcal{I}$. Then $\bigcup_{i\in\mathcal{I}} E_i$ is countable.* More glibly, it can also be stated as follows: *A countable union of countable sets is countable.*

We will now use this theorem to prove the countability of the set of all rational numbers. It has been already proved that the set $\mathbb{Q} \cap [0, 1]$ is countable. Similarly, it can be showed that $\mathbb{Q} \cap [n, n+1]$ is countable, $\forall n \in \mathbb{Z}$. Let $Q_i = \mathbb{Q} \cap [i, i + 1]$. Thus, clearly, the set of all rational numbers, $\mathbb{Q} = \cup_{i\in\mathbb{Z}} Q_i$ – a countable union of countable sets – is countable.

Remark: For two finite sets A and B, we know that if A is a strict subset of B, then B has cardinality greater than that of A. As the above examples show, this is not true for infinite sets. Indeed, $\mathbb{N}$ is a strict subset of $\mathbb{Q}$, but $\mathbb{N}$ and $\mathbb{Q}$ are equicardinal!

4. The set of all *algebraic* numbers (numbers which are roots of polynomial equations with rational coefficients) is countable.

5. The set of all computable numbers, i.e., real numbers that can be computed to within any desired precision by a finite, terminating algorithm, is countable (see Wikipedia article for more details).

Definition 3.8 *A set F is* **uncountable** *if it has cardinality strictly greater than the cardinality of* $\mathbb{N}$.

In the spirit of Definition 3.5, this means that F is uncountable if an injective function from $\mathbb{N}$ to F exists, but no such bijective function exists.

An interesting example of an uncountable set is the set of all infinite binary strings. The proof of the following theorem uses the celebrated 'diagonal argument' of Cantor.

Theorem 3.9 (Cantor) *: The set of all infinite binary strings, $\{0,1\}^\infty$, is uncountable.*

Proof: It is easy to show that an injection from $\mathbb{N}$ to $\{0,1\}^\infty$ exists (exercise: produce one!). We need to show that no such bijection exists.

Let us assume the contrary, i.e, let us assume that the set of all binary strings, $A = \{0,1\}^\infty$ is countably infinite. Thus there exists a bijection $f : A \to \mathbb{N}$. In other words, we can order the set of all infinite binary strings as follows:

$$\begin{array}{cccccc} a_{11} & a_{12} & a_{13} & . & . & . \\ a_{21} & a_{22} & a_{23} & . & . & . \\ a_{31} & a_{32} & a_{33} & . & . & . \\ . & . & . & & & \\ . & . & . & & & \\ . & . & . & & & , \end{array} \quad \text{where, } a_{ij} \text{ is the } j^{th} \text{ bit of the } i^{th} \text{ binary string, } i,j \geq 1.$$

Consider the infinite binary string given by $\bar{a} = \bar{a_{11}}\bar{a_{22}}\bar{a_{33}}...$, where $\bar{a_{ij}}$ is the complement of the bit a_{ij}.

Since our list contains *all* infinite binary strings, there must exist some $k \in \mathbb{N}$ such that the string $\bar{a}$ occurs at the k position in the list, i.e., $f(\bar{a}) = k$. The k^{th} bit of this specific string is $\bar{a_{kk}}$. However, from the above list, we know that the k^{th} bit of the k^{th} string is a_{kk}. Thus, we can conclude that the string $\bar{a}$ cannot occur in any position $k \geq 1$ in our list, contradicting our initial assumption that our list exhausts all possible infinite binary strings.

Thus, there cannot possibly exist a bijection from $\mathbb{N}$ to $\{0,1\}^\infty$, proving that $\{0,1\}^\infty$ is uncountable. ■

Now using Cantor's theorem, we will prove that the set of irrational numbers is uncountable.

Claim 3.10 *The sets $[0,1]$, $\mathbb{R}$ and $\{\mathbb{R} \setminus \mathbb{Q}\}$ are uncountable.*

Proof: Firstly, consider the set $[0,1]$. Any number in this set can be expressed by its binary equivalent and thus, there appears to be a bijection from $[0,1] \to \{0,1\}^\infty$. However, this is not exactly a bijection as there is a problem with the dyadic rationals (i.e., numbers of the form $\frac{a}{2^b}$, where a and b are natural numbers, and a is odd). For example, 0.01000.... in binary is the same as 0.001111.... . However we can tweak this "near bijection" to produce an explicit bijection in the following way. For any infinite binary string $x = (x_1, x_2, \dots) \in \{0,1\}^\infty$, let

$$g(x) = \sum_{k=1}^{\infty} x_k 2^{-k}.$$

The function g maps $\{0,1\}^\infty$ "almost bijectively" to $[0,1]$, but unfortunately, the dyadic rationals have two pre-images. For example we have $g(1000...) = g(0111...) = \frac{1}{2}$. To fix this let the the set of dyadic rationals be diven by the list

$$\mathcal{D} = \left\{ d_1 = \frac{1}{2}, d_2 = \frac{1}{4}, d_3 = \frac{3}{4}, d_4 = \frac{1}{8}, d_5 = \frac{3}{8}, d_6 = \frac{5}{8}, d_7 = \frac{7}{8}, ... \right\}$$

Note that the dyadic rationals can be put in a list as given above as they are countable. Next, we define the following bijection $f(x)$ from $\{0,1\}^\infty$ to $[0,1]$.

$$f(x) = \begin{cases} g(x) & \text{if } g(x) \notin \mathcal{D}, \\ d_{2n-1} & \text{if } g(x) = d_n \text{ for some } n \in \mathbb{N} \text{ and } x_k \text{ terminates in 1}, \\ d_{2n} & \text{if } g(x) = d_n \text{ for some } n \in \mathbb{N} \text{ and } x_k \text{ terminates in 0}. \end{cases}$$

This is an explicit bijection from $\{0,1\}^\infty$ to $[0,1]$ which proves that the set $[0,1]$ is uncountable. (Why?)

Next, we can define a bijection from $(0,1) \to \mathbb{R}$, for instance using the function $\tan(\pi x - \frac{\pi}{2}),\ x \in (0,1)$. Thus the set of all real numbers, $\mathbb{R}$ is uncountable.

Finally, we can write, $\mathbb{R} = \mathbb{Q} \cup \{\mathbb{R} \setminus \mathbb{Q}\}$. Since $\mathbb{Q}$ is countable and $\mathbb{R}$ is uncountable, we can easily argue that $\{\mathbb{R} \setminus \mathbb{Q}\}$, i.e, the set of all irrational numbers, is uncountable. ■

3.3 Exercises

1. Prove that $2^{\mathbb{N}}$, the power set of the natural numbers, is uncountable. (Hint: Try to associate an infinite binary string with each subset of $\mathbb{N}$.)

2. Prove that the Cartesian product of two countable sets is countable.

3. Let A be a countable set, and B_n be the set of all n-tuples $(a_1, ..., a_n)$, where $a_k \in A (k = 1, 2, ..., n)$ and the elements $a_1, a_2, ..., a_n$ need not be distinct. Show that B_n is countable.

4. Show that an infinite subset of a countable set is countable.

5. A number is said to be an algebraic number if it is a root of some polynomial equation with integer coefficients. For example, $\sqrt{2}$ is algebraic since it is a root of the polynomial $x^2 - 2$. However, it is known that π is not algebraic. Show that the set of all algebraic numbers is countable. Also, a transcendental number is a real number that is not algebraic. Are the transcendental numbers countable?

6. The *Cantor* set is an interesting subset of [0, 1], which we will encounter several times in this course. One way to define the Cantor set C is as follows. Consider the set of all real numbers in $[0,1]$ written down in ternary (base-3) expansion, instead of the usual decimal (base-10) expansion. A real number $x \in [0,1]$ belongs to C iff x admits a ternary expansion without any 1s. Show that C is uncountably infinite, and that it is indeed equi-cardinal with $[0,1]$.

References

[1] Walter Rudin, "Principles of Mathematical Analysis," *McGraw Hill International Series*, Third Edition.