MATH 215 Mathematical Analysis, Spring 2012

Handout 2: Further Notes on Countability

Laurence Barker, Mathematics Department, Bilkent University,
version: 1 March 2012.

These notes are merely a supplement to the course text:

Walter Rudin, *Principles of Mathematical Analysis*, 3rd Edition, (McGraw-Hill, 1976).

Summary of definitions and preliminary results

Given sets X and Y, we write $|X| \leq |Y|$ provided there exists an injection $X \to Y$. When $|X| \leq |Y|$ and $|Y| \leq |X|$, we write $|X| = |Y|$.

We call $|X|$ the **cardinality** of X. It is to be understood that $|X|$ is a mathematical object called a **cardinal number**. We make the identification $n = |\{1, 2, ..., n\}|$. A set X is said to be **finite** provided it can be written in the form $X = \{x_1, ..., x_n\}$ where the elements x_1, ..., x_n are mutually distinct. For such X, the cardinality of X, also called the **size** of X, is understood to be $|X| = n$. It is also to be understood that the empty set $\emptyset$ is a finite set with size $|\emptyset| = 0$. Thus, the cardinalities of the finite sets are the natural numbers.

We say that X is **countable** provided $|X| \leq |\mathbb{N}|$, in other words, provided there exists an injection $f : X \to \mathbb{N}$. In that case, we can enumerate the elements of X as x_0, x_1, ... in such a way that $f(x_0) < f(x_1) < ....$ Plainly, every finite set is countable. As a piece of jargon, when X is countable and infinite, we say that X is **countably infinite**. It is not hard to see that X is countably infinite if and only if $|X| = |\mathbb{N}|$.

Remark 1: *Let X, Y, Z be sets and let $f : X \to Y$ and $g : Y \to Z$ be functions. Consider the composite function $g \circ f : X \to Z$.*
(1) *If f and g are injective, then $g \circ f$ is injective.*
(2) *If f and g are surjective, then $g \circ f$ are surjective.*
(3) *If f and g are bijective, then $g \circ f$ is bijective.*

Proof: Suppose that f and g are injective. Given $x, x' \in X$ with $x \neq x'$ then $f(x) \neq f(x')$ by the injectivity of f, whence $g(f(x)) \neq g(f(x'))$ by the injectivity of g. We have shown that $g \circ f$ is injective. Part (1) is established.

Now suppose that f and g are surjective. Given $z \in Z$ then, since g is surjective, we have $z = g(y)$ for some $y \in Y$. Since f is surjective, $y = f(x)$ for some $x \in X$. We have $z = g(f(x))$, so $g \circ f$ is surjective. Part (2) is established.

Part (3) is immediate from parts (1) and (2). $\square$

The remark implies that, given sets X, Y, Z with $|X| \leq |Y|$ and $|Y| \leq |Z|$, then $|X| \leq |Z|$.

Proposition 2: *Given sets X and Y with $X \neq \emptyset$, then $|X| \leq |Y|$ if and only if there exists a surjection $Y \to X$.*

Proof: Suppose that $|X| \leq |Y|$, in other words, there exists an injection $f : X \to Y$. Since $X \neq \emptyset$, we can choose an element $x_0 \in X$. Let $g : Y \to X$ be the function such that $g(y) = x$ when $y = f(x)$ while $g(y) = x_0$ when y is not in the image of f. Plainly, y is surjective.

Conversely, if there exists a surjection $g : Y \to X$ then, for each $x \in X$, we can choose an element $f(x) \in Y$ such that $g(f(x)) = x$. The function $f : X \to Y$ is plainly injective. $\square$

For a set X, the **power set** $\mathcal{P}(X)$ is defined to be the set of all subsets of X. It is easy to see that, if X is finite, then $|\mathcal{P}(X)| = 2^{|X|}$ and, perforce, $|X| < |\mathcal{P}(X)|$. The next result says that the conclusion still holds for arbitrary sets.

Theorem 3: (Cantor) *Given a set X, then $|X| < |\mathcal{P}(X)|$.*

Proof: We have $|X| \leq |\mathcal{P}(X)|$ because the function sending each element $x \in X$ to the element $\{x\} \in \mathcal{P}(X)$ is injective. For a contradiction, suppose that $|X| = |\mathcal{P}(X)|$. Since $\mathcal{P}(X) \neq \emptyset$, Proposition 2 implies that there exists a surjection $f : X \to \mathcal{P}(X)$. Let

$$A = \{x \in X : x \notin f(x)\} .$$

Choose an element $a \in X$ such that $f(a) = A$. The conditions $a \in A$ and $a \notin A$ imply each other, which is absurd. $\square$

It follows, in particular, that the set $\mathcal{P}(\mathbb{N})$ is uncountable.

Some comments on the notion of proof

A proof is a very clear deductive explanation.

In particular, a proof is something communicated from one person to another person.

So the validity of a proof depends on the audience.

In this course, the audience are the students. So an argument is a proof if it would persuade those students who have mastered the appropriate prerequisites. (Incidentally, that is my criterion when marking exams.)

By that criterion, some of my own arguments, presented during the course, will not be proofs. No doubt, some of the arguments produced by students, too, will not be proofs. That will not matter. Mathematics is discipline where important mistakes tend to get detected and then corrected.

Perhaps, the above justification of Remark 1 is not a proof. If Remark 1 was obvious already, then no persuasion was involved, and it would follow that the argument I presented could not have been a proof.

Probably, Proposition 2 really did need some justification. Still, the argument I gave was not very interesting.

Unquestionably, Theorem 3 has some genuine content. The notion of proof is important because of results like this. So, if the argument I gave for Theorem 3 is not a proof, then there are some important corrections that we need to make.

Some standard results

The following results are standard, which is to say, they are known by all mathematically competent people who have studied the topic.

For that reason, you may assume them in an exam question, except when the question makes it clear that their proofs are required.

It is important to learn proofs of these results. Proofs of theorems tend to be more general that statements of theorems. In applications, it often happens that one cannot directly apply known theorems but, instead, one can adapt the ideas behind the proofs of the theorems.

For all except one of the next five results, proofs were given in class.

Remark 4: *Let X be a subset of a set Y. Then $|X| \leq |Y|$. In particular, if Y is countable then X is countable.*

Proposition 5: *A countable union of countable sets is countable. That is to say, given a countable set I, and countable sets A_i for each $i \in I$, then the union $\bigcup_{i \in I} A_i$ is countable.*

Proof: We may assume that $I = \mathbb{N}$. Let p_0, p_1, ... be an enumeration of the primes. For each $i \in \mathbb{N}$, let f_i be an injection $A_i \to \mathbb{N}$. Write $A = \bigcup_i A_i$. Given $a \in A$, let i be the smallest natural number such that $a \in A_i$, and let $f(a) = p_i^{f_i(a)}$. By unique prime factorization, f is an injection $A \to \mathbb{N}$. $\square$

Proposition 6: *A finite direct product of countable sets is countable. That is, given countable sets A_1, ..., A_n, then the direct product $A_1 \times ... \times A_n$ is countable.*

Theorem 7: *The set of rational numbers $\mathbb{Q}$ is countable.*

Theorem 8: *The set of real numbers $\mathbb{R}$ is uncountable.*

Some material not on the examinable syllabus

The two theorems in this section are worth noting because, together, they clarify the notion of a cardinal number. However, we shall not be making use of them in the course, so they are excluded from the examinable syllabus.

Proof of the next result is elementary but somewhat complicated.

Bernstein–Cantor–Schröder Theorem: *Given sets X and Y such that $|X| = |Y|$, then there exists a bijection $X \to Y$.*

Note that this is a subtle theorem, not at all obvious. The assumption $|X| = |Y|$ is that there exists an injection $X \to Y$ and an injection $Y \to X$. Excluding the trivial case where $Y = \emptyset$, this is equivalent to the condition that there exists an injection $X \to Y$ and a surjection $X \to Y$. It is not at all straightforward to get from there to the conclusion that there exists a bijection between X and Y.

Proof of the next theorem requires some deeper set theory. In fact, it requires the Axiom of Choice. Some tricky philosophy is required and, really, the only way to establish this result properly is to define the notion of a set axiomatically.

Trichotomy Theorem: (Cantor) *Given sets X and Y, then exactly one of the following three conditions holds: $|X| < |Y|$; or $|X| = |Y|$; or $|X| > |Y|$.*

Another motive for the axiomatic definition of a set is that, all systematic approaches that are powerful enough for normal mathematics lead to counter-intuitive conclusions. And cavalier approaches lead to paradoxes.

Russell's Paradox: *Let S be the set whose elements are those sets T such that $T \notin T$. Then the statements $S \in S$ and $S \notin S$ are the negations of each other, yet they imply each other.*

Let us mention that Cantor introduced two different systems of numbers that could be applied to infinite sets: the *ordinal numbers* and the *cardinal numbers*. The ordinal numbers are no longer considered to be of importance, because their main purpose (a generalization of the Principle of Mathematical Induction) has been superceded by superior techniques (Zorn's Lemma). The notion of the cardinal numbers, though, is fundamental to much of mathematics.

Anyway, that historical background indicates one reason why, for infinite sets, we tend to use the term *cardinality* rather than the more down-to-earth term *size*.

Homework 1

I have rephrased Question 1 because, when I set it for homework, we had not yet established Proposition 5. Questions 2, 3, 4 are from Rudin, page 45, at the end of Chapter 2.

1: Give a definition of a **countable set**. Directly from the definition you gave, show that a countable union of finite sets is countable. In other words, letting I be a countable set and letting A_i be a finite set for each $i \in I$, then the union $\bigcup_{i \in I} A_i$ is countable.

2: A complex number z is said to be **algebraic** provided there exist integers a_n, a_{n-1}, ..., a_1, a_0 such that $a_n \neq 0$ and $a_n z^n + a_{n-1} z^{n-1} + ... + a_1 z + a_0 = 0$. Show that the set of all algebraic numbers is countable. (Hint: for every positive integer m, there are only finitely many integers n and a_n, a_{n-1}, ..., a_1, a_0 such that $n + |a_n| + |a_{n-1}| + ... + |a_1| + |a_0| = m$.)

3: Prove that there exist real numbers that are not algebraic.

4: Is the set of all irrational numbers countable?

Solutions 1

1: A set X is said to be **countable** provided X has the form $X = \{x_0, x_1, ...\}$ where x_0, x_1, ... is a finite or infinite sequence.

We are to show that, given sets A_0, A_1, ..., then the union $A_0 \cup A_1 \cup ...$ is countable. Inductively, suppose we have enumerated the elements of $A_0 \cup ... \cup A_k$ as a_0, ..., a_{m_k}. Then we can enumerate the elements of $A_{k+1} - (A_0 \cup ... \cup A_k)$ as a_{m_k+1}, ..., $a_{m_{k+1}}$.

Comment A: Alternatively, one could adapt the proof of Proposition 5.

Comment B: It is implicit from the phrasing of Question 1 that you are required to prove this standard result, and that you may not simply invoke Proposition 5.

2: For each positive integer m, let A_m be the set consisting of the complex numbers z such that $a_n z^n + ... + a_1 z + a_0 = 0$ for integers a_n, ..., a_0 satisfying $n + |a_n| + ... + |a_0| = m$. Given m, then there are only finitely many integers n and a_n, a_{n-1}, ..., a_1, a_0 satisfying $n + |a_n| + ... + |a_0| = m$. Furthermore, given n, a_n, ..., a_0, then there are at most n complex numbers satisfying $a_n z^n + ... + a_1 z + a_0 = 0$. Therefore A_m is finite. The set of algebraic integers is the union $\bigcup_{m=1}^{\infty} A_m$ and, by Question 1, this union is countable.

Comment C: In the latest argument, did we really need to explain why each A_m is finite, or was it obvious? Well, that is a moot question, and it is not very important anyway. If we were to omit just that part of the explanation, then all the key ideas in the proof would still be communicated to the reader.

3: Let A be the set of algebraic integers. In the previous question, we showed that A is countable. Perforce, $A \cap \mathbb{R}$ is countable. But $\mathbb{R}$ is uncountable. Therefore $A \cap \mathbb{R} \neq \mathbb{R}$.

4: Let I be the set of all irrational numbers. Then $\mathbb{R} = \mathbb{Q} \cap I$. But $\mathbb{Q}$ is countable and the union of two countable sets is countable. Yet $\mathbb{R}$ is uncountable. So I must be uncountable.