

Math 101  
Solution and Commentary  
for the Second Group Project

Stefan Karpinski

January 6, 2000

**Part 1.** If  $A$  and  $B$  are countable then we can index them by  $\mathbb{N}$

$$\begin{aligned}A &= \{a_0, a_1, \dots\} \\ B &= \{b_0, b_1, \dots\}.\end{aligned}$$

Then we can define

$$c_n = \begin{cases} a_{n/2} & \text{if } 2 \mid n, \\ b_{(n-1)/2} & \text{if } 2 \nmid n. \end{cases}$$

Then because  $A$  and  $B$  are distinct, we know that all the  $c_n$  are distinct. Thus we have shown that we can index  $A \cup B$  by  $\mathbb{N}$  simply as

$$A \cup B = \{c_0, c_1, \dots\}.$$

**Part 2.** If we enumerate  $A$  and  $B$  as above, we can write out the elements of  $A \times B$  in an infinite "table"

$$\begin{array}{cccc} (a_0, b_0) & (a_0, b_1) & (a_0, b_2) & \dots \\ (a_1, b_0) & (a_1, b_1) & (a_1, b_2) & \dots \\ (a_2, b_0) & (a_2, b_1) & (a_2, b_2) & \dots \\ \vdots & \vdots & \vdots & \ddots \end{array}$$

Then we can enumerate the entire table by traversing diagonals up and left repeatedly

$$A \times B = \{(a_0, b_0), (a_1, b_0), (a_0, b_1), (a_2, b_0), (a_1, b_1), (a_0, b_2), \dots\}$$

Thus  $A \times B$  is countable.

**Part 3.** The idea of the proof is that we begin with any list of decimal expansions of reals in the interval  $(0, 1)$ :

$1 \mapsto 0.123456789\dots$   
 $2 \mapsto 0.7\underline{1}7777777\dots$   
 $3 \mapsto 0.31\underline{4}159265\dots$   
 $4 \mapsto 0.100000000\dots$   
 $5 \mapsto 0.2468\underline{1}0121\dots$   
 $\vdots$

Whatever we may have crammed onto this list in whatever clever way we may have constructed it, we can always construct a decimal which is not on this list by going down the diagonal and changing each digit. This may be achieved more specifically by taking the not-necessarily-new diagonal decimal  $d$  (in this case  $d = 0.17401\dots$ , with digits those underlined above) and changing each of its digits, so that the new number given is different from the  $n$ th listed decimal at the  $n$ th decimal place, so that our new number cannot be on the list we started with. For example, we could take our new decimal  $n = 0.25319\dots$  in this case.

There are two annoying problems to be addressed (and they both stem from the essential flaw with decimal expansion which makes decimals usually more irritating and painful to deal with in abstract mathematics than is worthwhile for the conceptual ease they afford): while we know by the principle of nested closed intervals for the real line that every decimal expansion corresponds to a real number, this correspondence is *not* injective (but it is surjective). It doesn't fail by very much, but the failure is enough to make things really annoying. The problem is that we have

$$\begin{aligned}
 1.\overline{0} &= 0.\overline{9} \\
 0.12345679\overline{0} &= 0.12345678\overline{9}
 \end{aligned}$$

where the overline means that those digits (only one in each case here) repeat forever. Fortunately these are the only cases—the worst that injectivity ever fails is by sending two decimal expansions to the same real number, never three of four or more—and only pairs of otherwise matching numbers ending in repeating 0 or 9 will get paired like this. So the fear is that while our new decimal expansion  $n$  may not be one of the decimal expansions on the list, it might represent the same real number in  $(0, 1)$  as one of the decimals on the list. We can fix this by never changing the digit 0 in  $d$  to 9 in  $n$  and vice versa. (Convince yourself that this fixes the problem.)

The other problem is that we could conceivably end up with  $n = 0.9999\dots$ , which is not in  $(0, 1)$  at all so we have not even produced the decimal expansion of a new real number in  $(0, 1)$ . This is of course related to the previous problem but is not *a priori* fixed by the solution to the other problem. However, we don't need to change our procedure at all, we merely need assert that our list

of decimal expansions must begin with say  $0.9000\dots$ , so that  $n = 0.9999\dots$  becomes impossible. This does not affect our proof that  $(0, 1)$  is uncountable since if we were hoping to list all the reals in  $(0, 1)$  then  $0.9$  will surely be in that list at some point. All we've done here is move it to the front of the list which is clearly harmless.

—beginning of rant and rave—

These nitpicking, silly little problems and their inelegant fixes are one of the reasons why no one uses decimal expansions in mathematics. It's just messy. Moreover, if we're dealing with a rational number then, while we know that we can write out an exact decimal expansion for that number (allowing repeating digits at the end, which is also messy of course), fractional form (especially reduced fractional form) tells us far more about the mathematical properties of that number than the decimal form does. If we're dealing with an irrational number then we can't even hope to write out an exact decimal expansion (since the expansion never terminates and never repeats), whereas most of the irrationals that one deals with are expressible exactly with radicals (possibly nested radicals). There are so few numbers which occur often but aren't exactly expressible that we have simply named the most important ones:  $\pi$ ,  $e$ —and I can't even think of any more.

The question of which algebraic numbers—i.e. numbers which are roots of rational polynomials—can and cannot be expressed exactly with radicals is a very interesting one which is answered using Galois Theory in Math 123. This is widely considered some of the most beautiful material in all of mathematics, and is really worth taking if you have the time and the interest. Math 122 is absolutely wonderful stuff too: groups, rings, fields and the better parts of linear algebra (216 is definitely the worse parts of linear algebra).

The one advantage that decimal representation does offer, which is precisely what makes it so popular with everyone besides mathematicians, is that it lets you immediately tell how big the number in question is. You can immediately see which two integers it lies between, and which tenths of integers, etc. In the real world we don't really care about exact expressions for insoluble algebraics (algebraic numbers which cannot be expressed with radicals) or even about the number-theoretic properties of rational numbers. Numbers are for most people just a way of measuring how big things are. So we want primarily to be able to tell how big our numbers are as easily and quickly as possible. Decimals allow precisely that.

—end of rant and rave—

The colors of the spectrum as conventionally thought of form a continuum and hence have the cardinality of the continuum—i.e. the real numbers. Whether the actually are a continuum of possible colors is a question which quantum mechanics throws into doubt and I don't really know enough about the matter to say whether color is completely quantized or whether there are bits of uncountable continuum in the spectrum. On the other hand, we can

list all possible words written in the standard Roman alphabet (or any other finite alphabet for that matter) in what is known as lexicographic order. Lexicographic order begins with words of length 0—there’s only one, the empty string (and we’re not really considering it here), then words of length 1—there are  $k$  of them if our alphabet has  $k$  symbols—then the  $k^2$  words of length 2, etc. Since there are only finitely many words of a given length, we will eventually get to all of the words of any length. So there must be only countably many possible names for colors. The obvious conclusion is that we could never possibly name all the colors of the spectrum even if we were somehow able to define an infinite number of color names.

**Part 4.** The algebraic numbers are countable. To show this, we begin by showing that there are only countably many polynomials with rational coefficients. We can list the rational polynomials. To do this we consider a polynomial as a “word” spelled out by its coefficients. A word of length  $n$  corresponds to a polynomial of degree  $n$  (the degree of a non-constant polynomial is the greatest power of  $x$  with non-zero coefficient; the degree of a constant polynomial is 0). However we cannot use lexicographic order since the “alphabet” in this situation is  $\mathbb{Q}$  and is not finite so there are no longer only finitely many words of a given length. However, there are only countably many words of a given length (since the set of words of length  $n$  with alphabet  $A$  is just the set of ordered  $n$ -tuples and elements of  $A$ —i.e.  $A^n = A \times \cdots \times A$ —which is countable). Suppose that we write  $p_{n,m}$  for the  $m$ th polynomial of degree  $n$ . Then we can write all of the rational polynomials in a table:

$$\begin{array}{cccc}
 p_{0,1} & p_{0,2} & p_{0,3} & \dots \\
 p_{1,1} & p_{1,2} & p_{1,3} & \dots \\
 p_{2,1} & p_{2,2} & p_{2,3} & \dots \\
 \vdots & \vdots & \vdots & \ddots
 \end{array}$$

From here we can list them all as before by traversing diagonals up and right:

$$p_{0,1} \ p_{1,1} \ p_{0,2} \ p_{2,1} \ p_{1,2} \ p_{0,3} \ \dots$$

So, having established that the rational polynomials themselves are countable we use this to show that the algebraic numbers—i.e. the roots of rational polynomials—are also countable. Each polynomial of degree  $n$  has at most  $n$  different roots in the complex plane. So in our previous list, we can just replace each polynomial by the list of its roots and get a list of all the possible roots of polynomials. The only consideration is that each algebraic number is listed repeatedly (a lot of times—i.e. infinitely many times each). However, that’s not a problem since we’ve produced a surjection from the natural numbers to the algebraic numbers, which is sufficient to show countability of the algebraic numbers. We already know that  $\mathbb{R}$  is uncountable and now we’ve established that  $\mathbb{A}$  (the standard notation for the algebraic numbers) is countable, so  $\mathbb{R} - \mathbb{A}$ —the transcendental numbers—must be uncountable to account for the missing

stuff (like the black matter in the universe that the cosmologists are scrambling to find).

**Part 5.** Let  $A$  be a set. Suppose that we have a surjection  $f: A \rightarrow 2^A$ . (Here, as usual,  $2^A$  denotes the power set of  $A$ .) Then we may consider the set

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

$T \in 2^A$  (since  $T \subseteq A$ ) and  $f$  is surjective so there exists  $t \in A$  such that  $f(t) = T$ . The killer question is “is  $t$  an element of  $T$  or not?” If it is then it shouldn’t be and if it isn’t then it should be. This is the quintessential contradiction. Cantor, you genius.

**Part 6.** The identity function on a given set shows reflexivity of  $\sim$ . Since the composition of bijections is a bijection,  $\sim$  is also transitive. Finally,  $\sim$  is symmetric since bijections are invertible and the inverse of a bijection is also a bijection.

To put it mildly, there are **a lot** of cardinals. There are so many cardinals that the cardinals cannot be put into a set. If we could form the set of all cardinals then what we would really have is a set containing a bunch of equivalence classes—i.e. sets—in which every possible set appears somewhere—including (and here’s the kicker) the presumed set of all cardinals. So we have a set being an element of one of its elements and that is the sort of problematic situation that is disallowed by every sane model of set theory including the “naive” one that we’ve been using in this class. Recall that this sort of situation is problematic because it allows the construction of things like “the set of all sets that don’t contain themselves” or whatever your favorite deviant non-set might be.

**Part 7.** It is quickly clear that  $\preceq$  is reflexive and transitive (by the same arguments as the first part of 6). A much deeper question is whether it satisfies the final property of partial orders: does  $A \preceq B$  and  $B \preceq A$  imply  $A \sim B$ ? The Schröder-Bernstein Theorem is the affirmative answer to this question.

An even deeper question is whether  $\preceq$  actually forms a total order on any collection of sets  $S$ . It requires an additional and somewhat controversial (though very widely accepted) axiom, known as the Axiom of Choice, to show that this is in fact the case and that any pair of sets are comparable by the  $\preceq$  relation.

**Part 8.** Sorry, I wrote this all out with  $X$  and  $Y$  instead of  $A$  and  $B$  and now I don’t want to change it so let  $f: X \rightarrow Y$  and  $g: Y \rightarrow X$  be injections and forget about  $A$  and  $B$ . Denote the elements of  $X$  which originate in  $X$  by  $X_X$  and those that originate in  $Y$  by  $X_Y$ . Denote the elements of  $X$  which have infinite ancestry by  $X_\infty$ . Similarly we define  $Y_X$ ,  $Y_Y$  and  $Y_\infty$ . Clearly these are all pairwise disjoint and moreover,

$$\begin{aligned} X &= X_X \cup X_Y \cup X_\infty \\ Y &= Y_X \cup Y_Y \cup Y_\infty. \end{aligned}$$

Now a little notation. If  $A \subseteq X$  and  $h: X \rightarrow Y$ , we write  $h|_A$  for the function  $h|_A: A \rightarrow Y$  that “agrees” with  $h$ . This is known as the restriction of  $h$  to  $A$ . If  $B \subseteq Y$  such that the image of  $h|_A$  is contained in  $B$  we may also write simply  $h|_A$  for the doubly restricted function  $h|_A: A \rightarrow B$ . (Doubly restricted since both its domain and range are restricted, not just the domain as in the previous case.) This is not technically the same function but restricting the range in this manner doesn’t really change anything essential about the function so we allow ourselves this convenient little notational ambiguity.

With this notation, we may observe that the functions

$$\begin{aligned} f|_{X_X} &: X_X \rightarrow Y_X \\ g^{-1}|_{X_Y} &: X_Y \rightarrow Y_Y \\ f|_{X_\infty} &: X_\infty \rightarrow Y_\infty \\ g^{-1}|_{X_\infty} &: X_\infty \rightarrow Y_\infty \end{aligned}$$

are all bijections with respective inverses

$$\begin{aligned} f^{-1}|_{Y_X} &: Y_X \rightarrow X_X \\ g|_{Y_Y} &: Y_Y \rightarrow X_Y \\ f^{-1}|_{Y_\infty} &: Y_\infty \rightarrow X_\infty \\ g|_{Y_\infty} &: Y_\infty \rightarrow X_\infty \end{aligned}$$

This is actually more functions than we need and we can “glue” them together in two different ways to get two possible obvious choices for bijections from  $X$  to  $Y$  (ok maybe they’re not that obvious):

$$h(x) = \begin{cases} f(x) & \text{if } x \in X_X \cup X_\infty, \\ g^{-1}(x) & \text{if } x \in X_Y. \end{cases}$$

or

$$k(x) = \begin{cases} f(x) & \text{if } x \in X_X, \\ g^{-1}(x) & \text{if } x \in X_Y \cup X_\infty. \end{cases}$$

These have inverse bijections

$$h^{-1}(y) = \begin{cases} f^{-1}(y) & \text{if } y \in Y_X \cup Y_\infty, \\ g(y) & \text{if } y \in Y_Y. \end{cases}$$

and

$$k^{-1}(y) = \begin{cases} f^{-1}(y) & \text{if } y \in Y_X, \\ g(y) & \text{if } y \in Y_Y \cup Y_\infty. \end{cases}$$

I know this may seem really confusing, but its not as bad as it seems. Just read it over again slowly and think about it for a while. Then take two Aspirin and call me in the morning.

**Part 9.** Rather than trying to directly produce a bijection between  $\mathbb{R}$  and  $2^{\mathbb{Z}^+}$ , I will instead produce an injection each way and then the Schröder-Bernstein Theorem (part 8) tells us how to make a bijection from this pair of injections.

First I'll cook up the injection from  $2^{\mathbb{Z}^+}$  into  $\mathbb{R}$ . A subset of  $\mathbb{Z}^+$  can be considered as a sequence of zeros and ones:

$$\begin{aligned} \{5\} &\longleftrightarrow (0, 0, 0, 0, 1, 0, 0, 0, \dots) \\ \{1, 3, 5, 7, \dots\} &\longleftrightarrow (1, 0, 1, 0, 1, 0, 1, 0, \dots) \\ \{2, 4, 6, 8, \dots\} &\longleftrightarrow (0, 1, 0, 1, 0, 1, 0, 1, \dots). \end{aligned}$$

The  $n$ th element of the sequence on the right is 1 if and only if  $n$  is an element of the set on the left. Well this is suddenly very suggestive of decimal expansions. We may make a function  $2^{\mathbb{Z}^+} \rightarrow \mathbb{R}$  by sending

$$\begin{aligned} \{5\} &\mapsto 0.00001000\dots \\ \{1, 3, 5, 7, \dots\} &\mapsto 0.10101010\dots \\ \{2, 4, 6, 8, \dots\} &\mapsto 0.01010101\dots \end{aligned}$$

If the decimal expansions are considered as binary "decimal" expansions (properly called just binary expansions) then this is not injective since it sends  $\{1\} \mapsto 0.1\bar{0}$  and  $\{2, 3, 4, \dots\} \mapsto 0.0\bar{1}$  but in binary  $0.1\bar{0} = 0.0\bar{1}$  so injectivity fails. But if we use any base besides 2, we no longer have this problem since  $0.1\bar{0} \neq 0.0\bar{1}$  in other bases.

Now we need an injection from  $\mathbb{R}$  to  $2^{\mathbb{Z}^+}$ . We know that  $\mathbb{Q}$  is countable so let  $f: \mathbb{Z}^+ \rightarrow \mathbb{Q}$  be a bijection. We know from the construction of the reals by Dedekind cuts that a real number is (by definition) uniquely identified by the set of rational numbers which are strictly less than it—i.e. its Dedekind cut. A Dedekind cut is a subset of  $\mathbb{Q}$  but via  $f$  we may turn it into a subset of  $\mathbb{Z}^+$ . This gives us an injective function from  $\mathbb{R}$  to  $2^{\mathbb{Z}^+}$ :

$$x \mapsto \{n \in \mathbb{Z}^+ : f(n) < x\}.$$

Convince yourself that this is injective.

I'm not sure what to say about the continuum hypothesis. It's famous. It's been proven unprovable. There's not much to say to that except "Wow. Crazy, man."

**Part 10.** You know the deal here.