Lecture 4

Ben Rosenberg

June 10, 2021

Cardinality (cont.)

From last time: We wanted to prove that the set of natural numbers was infinite. Recall that we needed some subset $E \subset \mathbb{N}$ of the natural numbers, an injection $f_1 : E \to \mathbb{N}$, and an injection $\mathbb{N} \to E$. By definition, this will prove that the set $\mathbb{N}$ is infinite.

Let E be the set of even natural numbers defined as $E = \{x \in \mathbb{N} | (\exists y \in \mathbb{N})(x = 2y)\}$. This is clearly a subset of $\mathbb{N}$.

Recall our parking lot analogy, in which an injection meant a one-to-one mapping of inputs to outputs, "telling the cars how to park." For our first injection, the license places are even numbers, and the parking spots are natural numbers. The easy way to do this for the first injection is with what is called the **identity injection**, in which we tell each car to go to its own parking spot. This can be represented as $f_1 : x \mapsto x$. When, in essence, we have an injection from a subset of a set to the set itself, the identity injection can be very useful.

Now we need to construct f_2. We can't use the same identity injection here, because there isn't a designated parking spot for cars with odd license plates. It looks like half of the cars cannot fit, because the parking spots are only even. But we can actually map each car using $f_2 : x \mapsto 2x$.

To prove that f_2 is an injection:

$$\begin{aligned} f_2(x) &= f_2(y) \\ 2x &= 2y \ (\text{ definition of } f_2) \\ x &= y \ (\text{ arithmetic – cancel } 2 \text{ because } 2 \neq 0) \end{aligned}$$

So, we have proven that this injection is valid.

The intuition for what we have done in this second injection is simply *stretching* the number line out by a factor of 2, so that each number in $\mathbb{N}$ is stretched out to reach the number two times itself.

The cardinality of E is the same as the cardinality of $\mathbb{N}$; we can simply rename the $0, 2, 4$, etc. to $0, 1, 2$, etc.

Notation: Cardinality of $\mathbb{N}$. We say that the cardinality of $\mathbb{N}$, $|\mathbb{N}|$, is equal to $\aleph_0$.

Theorem: There are no infinite sets with cardinality less than $\aleph_0$. (This is taken without proof.) In other words: If $|A| < |\mathbb{N}|$, then A is finite.

$\aleph_0$ is the *first* (smallest) infinite cardinality.

Definition: A set is **countable** if its cardinality is not greater than $\aleph_0$. Otherwise, it is **uncountable**. In other words, a set is countable if it is either finite or has cardinality $\aleph_0$.

The question is: are there sets that are uncountable? In other words – are there sets with cardinality $> \aleph_0$? The answer is yes. We are going to try to find a set that nobody can park.

Theorem: The union of countable sets is countable.

Consider the set of natural numbers. $\mathbb{N}$ is the disjoint union of E and D, with $E = \{x \in \mathbb{N} | (\exists y \in \mathbb{N})(x = 2y)\}$ and $D = \{x \in \mathbb{N} | (\exists y \in \mathbb{N})(x = 2y + 1)\}$. We know that $|E| = \aleph_0$ and $|D| = \aleph_0$. (We can find the second with the injection $x \mapsto 2x + 1$.) And $|E \cup D| = \aleph_0$, and $E \cap D = \emptyset$.

Say that: - $S_0 = \{x \in \mathbb{N} | (\exists y \in \mathbb{N})(x = 13 \cdot +0)\}$, - $S_1 = \{x \in \mathbb{N} | (\exists y \in \mathbb{N})(x = 13 \cdot +1)\}$, and so on, until - $S_1 2 = \{x \in \mathbb{N} | (\exists y \in \mathbb{N})(x = 13 \cdot +12)\}$.

There are thirteen possible remainders when a number is divided by 13, and each subset S_i of $\mathbb{N}$ is an infinite subset with cardinality equal to $\mathbb{N}$. We can thus split the natural numbers into any such parts without making their union into an uncountable set.

So, instead, let's try taking the product of sets to approach uncountability. As with our previous visualization of set product, draw out the coordinate plane with $\mathbb{N}$ on each of the axes. In order to make the points on the grid created by this Cartesian product, we can use a method that we can call zig-zagging (but which likely has a better mathematical name). Start by sending $0, 0$, and then proceed as shown in Figure 1.

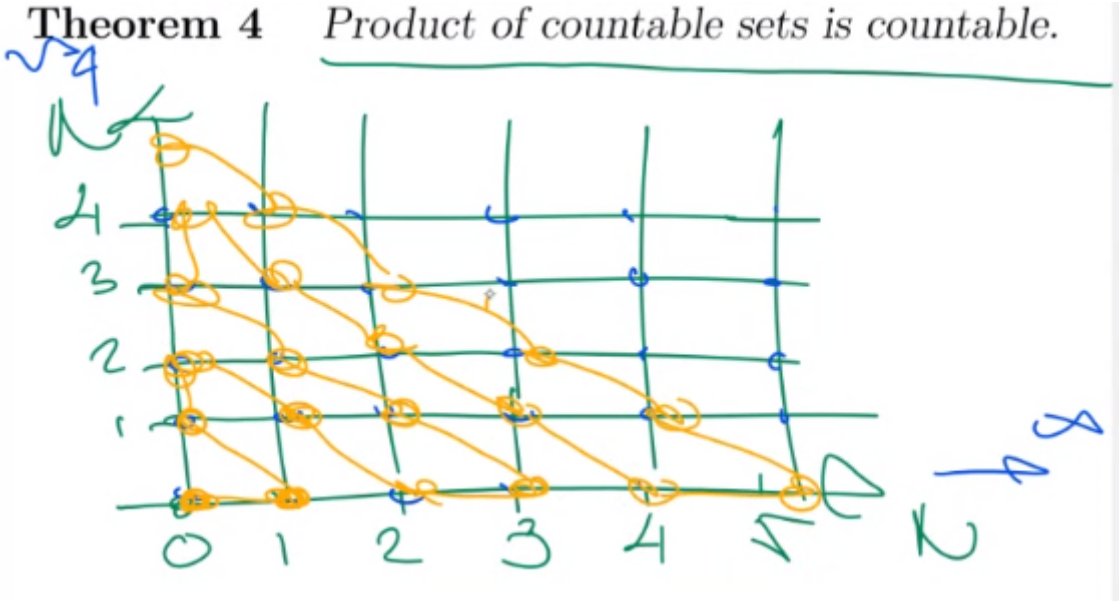

Figure 1: Zig-zagging across the coordinate plane

Gödel injection

Theorem: There exists an injection

$$\mathcal{G} : \bigcup_{k=1}^{\infty} \mathbb{N}^k \to \mathbb{N}.$$

This injection is called the **Gödel injection**.

Recall by the definition of exponentiation that $\mathbb{N}^k = \underbrace{\mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N}}_{k \text{ times}}$. As such, elements of $\mathbb{N}^k$ contain k different elements in their ordered tuple, and are k-tuples.

This union, $\bigcup_{k=1}^{\infty} \mathbb{N}^k$, is the set of all finite sequences of natural numbers.

Aside: Unbounded $\neq$ infinite

Infinite is as we defined above – it means something that contains a subset of equal cardinality; intuitively, it means something that has to contain, after renaming, the set of natural numbers.

Unbounded means finite, but without a fixed bound. This notion is relevant to the above-described injection as the sequences themselves are finite, but unbounded – *not* infinite.

Now: constructing the injection

Recall that cars may look like a sequence, somewhat like $x = [0, 1, 2, 79, 1056, 8, 1, 0]$ with cardinality $|x| = 8$ or $y = [0, 0, 0, 0, 0, 0, 1]$ with cardinality $|y| = 7$. We have to be able to park any such sequence, of every possible (finite) length and containing any natural numbers, that comes our way.

Theorem: Fundamental theorem of arithmetic: Every natural number greater than 1 can be written as a product of prime numbers in only one way.

Recall that a prime number is one which has no nontrivial divisors, and can only be divided by itself and 1.

Begin by writing out a table with one column having a natural number k, and the kth prime. There are infinitely many prime numbers, and so our table goes on forever, as shown in Figure 2.

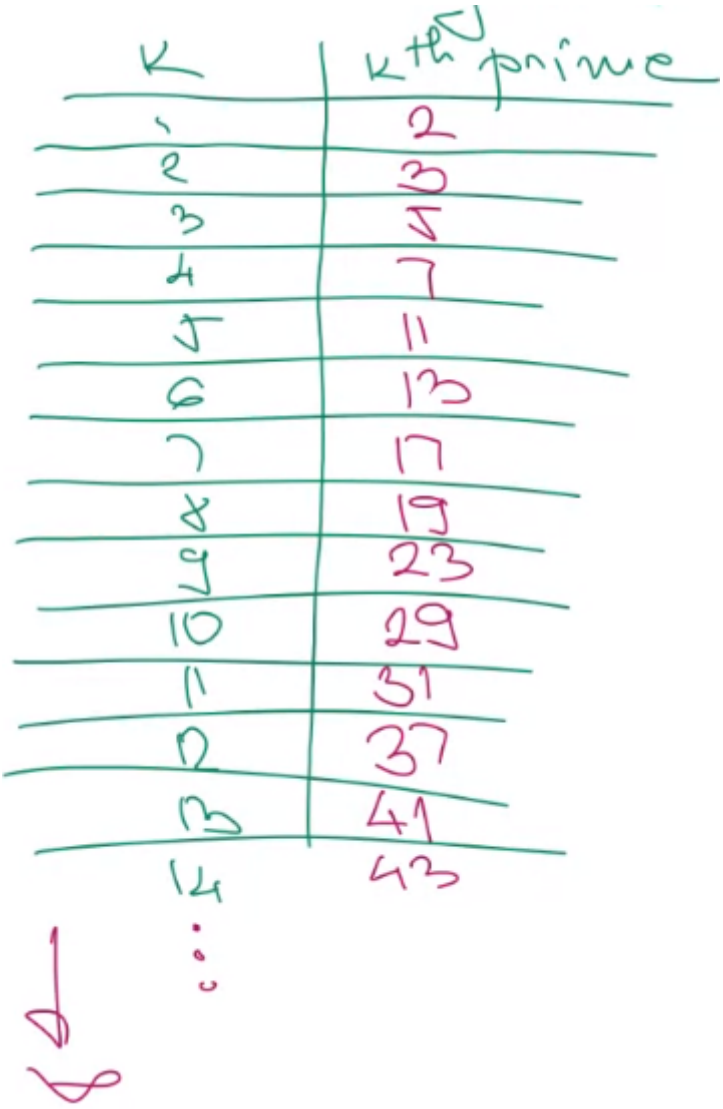

Figure 2: Table of prime numbers (may be slightly inaccurate)

Illustration of the fundamental theorem of arithmetic

Consider the number 72. We can represent this as the result of several different arithmetic operations:

- $72 = 50 + 22 = 16 + 30 + 20 + 6$ – this doesn't tell us much, because there are multiple different ways to add to 72
- $72 = 9 \cdot 8 = 2 \cdot 6 \cdot 4 = 18 \cdot 2 \cdot 2$ – this doesn't tell us much either because we don't necessarily know which numbers were multiplied
- 72 by multiplication of primes (construction from prime factors):
  - $72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$ – this is the only way in which we can obtain 72 *uniquely* by multiplication of prime factors (outside of permutations which we can ignore; there is only one way to represent 72 with prime factors).

Now, we can edit the number line to contain only the prime numbers. The question becomes, then: how many of each prime number should we assign to each location on the number line? For example, 72 has 3 2s and 2 3s.

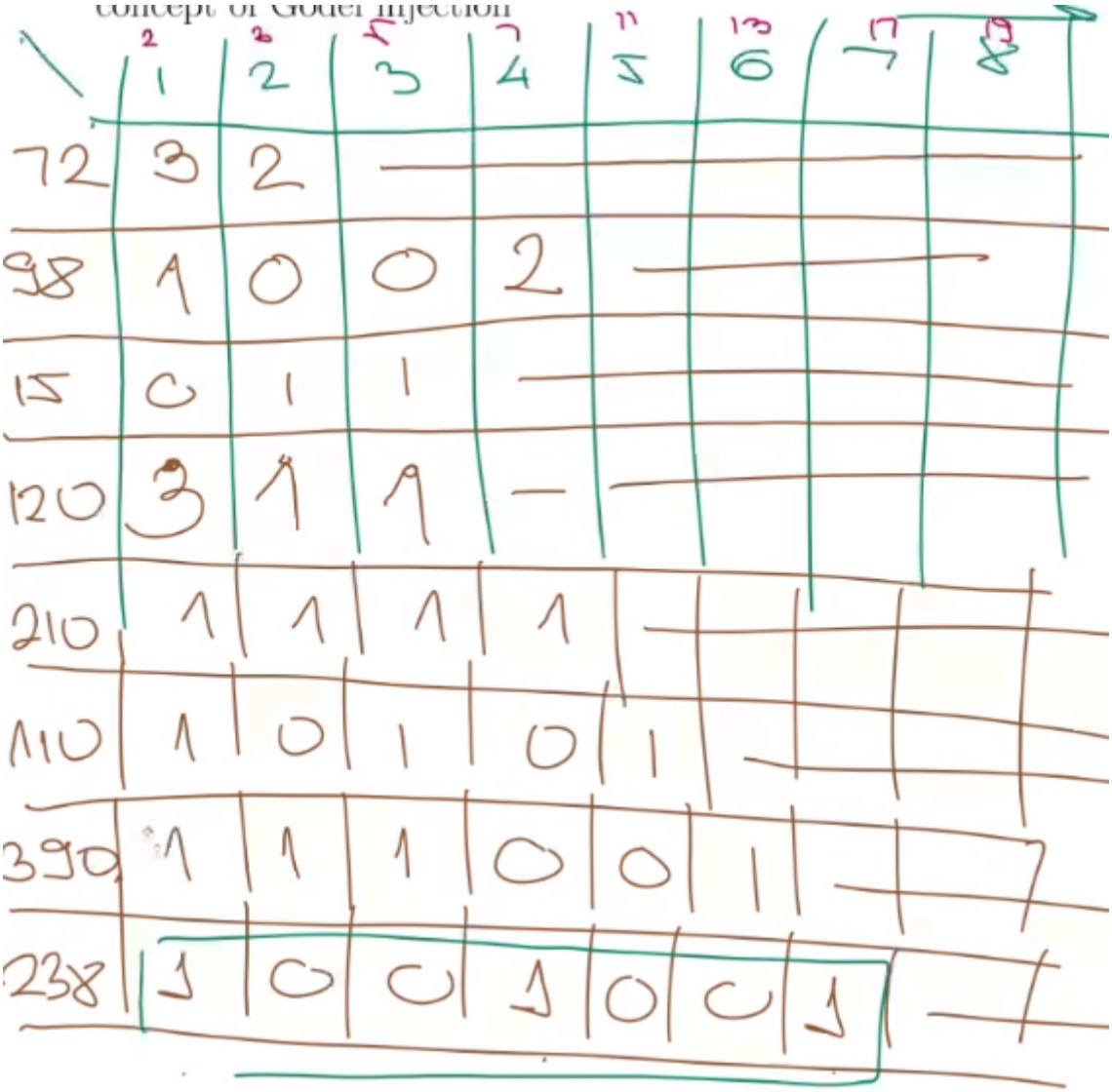

Figure 3: Prime factorization table

Problem: We don't have a way to represent 0 well.

- $[1] \to 2 = 2^1$
- $[1, 0] \to 2^1 \cdot 3^0 = 2$
- $[1, 0, 0] \to 2^1 \cdot 3^0 \cdot 5^0 = 2$

Since $n^0 = 1$, we lose the factor if we have zero as a sequence component.

The first way to go around this is to disallow zeroes on license plates, which is incorrect. The second way is to add one to every component in the sequence before mapping it, so that there are no zeroes and we can use the above approach correctly. We use this second approach in the following definition:

Definition: The **Gödel injection** is as follows:

$$\mathcal{G}(\langle x_1, x_2, ... x_k \rangle) = (\text{prime } \#1)^{x_1+1} \cdot (\text{prime } \#2)^{x_2+1} \cdot \cdots \cdot (\text{prime } \#k)^{x_k+1}$$

Now, we have:

- $[1] \to 2^{1+1} = 2^2 = 4$
- $[1, 0] \to 2^{1+1} \cdot 3^{0+1} = 12$
- $[1, 0, 0] \to 2^{1+1} \cdot 3^{0+1} \cdot 5^{0+1} = 60$

Notation: denote the Gödel number of a sequence x as $\mathcal{G}(x)$.

Inverse Gödel numbering:

- $\mathcal{G}^{-1}(2) = [0]$
- $\mathcal{G}^{-1}(4480) = ?$

The prime factorization of 4480 is $2^7 \cdot 5 \cdot 7$. But who parks here? Nobody. There is no sequence that can park here because there is no prime factor of 3 in its prime factorization. By definition, we need to use the first k primes in the Gödel number for a sequence of length k, each of which needs to have a positive exponent. 7, which is the largest prime in the factorization, is the fourth prime but there are only 3 different factors. As such, there is no sequence that corresponds to 4480 with inverse Gödel numbering.

The smallest of these such numbers, without a Gödel sequence, is 3. Also absent are 10 and 9, and 14. Each of these is missing at least one prime factor. In fact, there are infinitely many numbers which are not Gödel numbers.

- $\mathcal{G}^{-1}(720) = [3, 1, 0]$
  - The prime factorization of 720 is $2^4 \cdot 3^2 \cdot 5^1$.

Suppose we are given $\mathcal{G}^{-1}([x_1, x_2, x_3, x_4, x_5]) = n$. Then, n must be divisible by 10 as a 2 and a 5 appear. n is also divisible by 110, as it must have 2, 5, and 11. It is not divisible by 26 as the prime factorization of 26 is $2 \cdot 13$ and 13 is the 6th prime and the length of the sequence is 5.

Suppose we are given $\mathcal{G}^{-1}([x_1 + 1, x_2 + 2, x_3, x_4, x_5])$. Then, with our previous n, this is equal to $18n$ because we have an additional 2 3s and one more 2. Multiplying these together gives 18 as the factor by which n is being multiplied.

Suppose we are given $\mathcal{G}^{-1}([x_1 + 1, x_2 + 2, x_3, x_4, x_5, 1])$. Then, this is $n \cdot 13^{1+1} = n \cdot 13^2 = 169n$.

Back to uncountable sets

The Gödel injection existed, which foiled our plan to create an uncountable set. So, we want to continue trying to find an uncountable set – that is, a set with cardinality greater than $\aleph_0$.

Theorem: The set $\mathcal{P}(\mathbb{N})$ is uncountable.

Proof:

Assume that the above set is countable (for the sake of contradiction). Then, there must exist an injection from $f : \mathcal{P}(\mathbb{N}) \to \mathbb{N}$.

Aside: the basis for a proof by contradiction is the logical implication operation, in which a `false` conclusion means a `false` starting point (assumption), as long as the reasoning was correct.

Let $f_0 = f^{-1}(0)$ be the subset that parks at 0. Then, we might have the table shown in Figure 4.

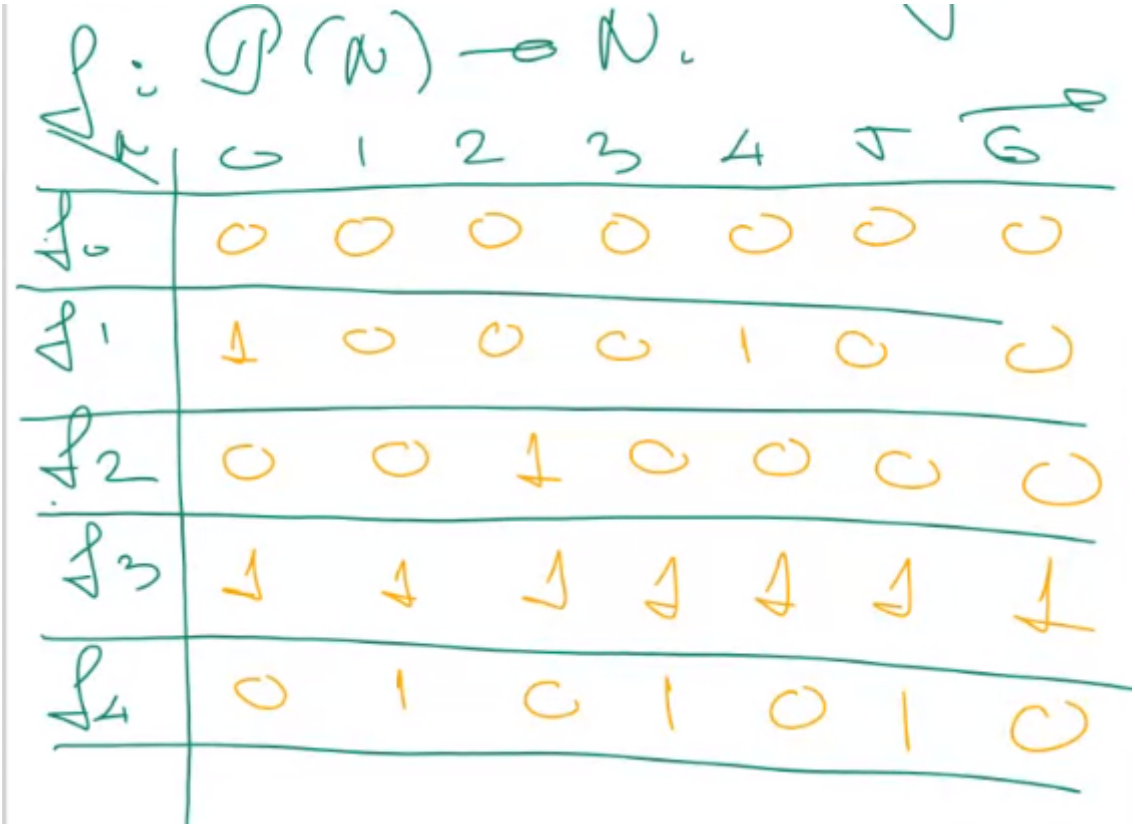

Figure 4: Presumed injection from $\mathcal{P}(\mathbb{N})$ to $\mathbb{N}$

Every subset of $\mathbb{N}$ must appear in the leftmost column – each must have its own row.

But now we can create our own subset, D, which is defined as follows:

(Aside: defining a set in $\mathbb{N}$ as above means to say whether each number is in it or not.)

We define D as $n \in D \Leftrightarrow n \notin f_n$. In other words, $n \in f_n \implies n \notin D$, and $n \notin f_n \implies m \in D$.

We are effectively going down the diagonal flipping and appending each of the digits therein, giving us the following D:

$$D = \{1, 1, 0, 0, 1, \dots\}$$

This is called **diagonalization**, and is the preferred (intuitive) method of proving that $\mathbb{N}$ is countable.

D is a subset of $\mathbb{N}$, and is therefore in $\mathcal{P}(\mathbb{N})$.

D must have its own row in the table called, say, α. Then, $D = f_\alpha$. The problem arises when we attempt to see whether the natural number α is in D. We know that if $\alpha \in D$, then $\alpha \notin f_\alpha$ by the definition of D. Then, by the definition of α, $\alpha \notin D$, which is a contradiction.

Consider the case in which we say that $\alpha \notin D$. Then, $\alpha \notin D \implies \alpha \notin f_\alpha$ by the definition of α, and then by the definition of D, $\alpha \in D$.

This is the crux of the *diagonalization argument*. We have clearly reached a contradiction, and therefore our initial assumption was wrong: $\mathcal{P}(\mathbb{N})$ must be uncountable; that is, $|\mathcal{P}(\mathbb{N})| = \aleph_1 > \aleph_0$. Further questions of cardinality are insofar as $\aleph_1$ is concerned are outside the scope of this course.

As a general method of proving things in this manner:

- Assume the structure exists
- Use the structure to construct an element which:
  - must belong to the structure
  - cannot belong to the structure, because we made it to differ from every element in the structure

Summary

- There are uncountably many languages (sets of strings)
- There are countably many strings (Gödel injection)

What is a program? A program is a text string, over some alphabet (ASCII-7, UTF-8, etc.). Therefore, there are countably many programs (the number of programs is $\aleph_0$).

How many problems are there? A problem is a set – a question, which asks whether $x \in S$. Example: How far will a hurricane go? The answer to this is as number (distance) that can be transformed into a sequence of bits:

$$\underbrace{\boxed{1|0|1|0|1|0|\cdots|0|1|0|1}}_{n \text{ bits}}$$

This is simply a collection of zeroes and ones, which are answers to `true`/`false` questions. There are then as many problems as there are sets, which means that there are uncountably many problems.

Therefore, there can never be a way to find a program for every problem.

DONE WITH CARDINALITY: EXAM ON MONDAY 6/14/2021