MATH 425a Problem Set 4

Qilin Ye

September 10, 2020

Problem 1. Let A and B be sets, and suppose that we have maps $f : A \to B$ and $g : B \to A$.

(1) If $g \circ f$ is injective, is f necessarily injective? What about g?

(2) If $g \circ f$ is surjective, is f necessarily surjective? What about g?

(3) If f is injective and g surjective, is $g \circ f$ necessarily injective? Surjective?

(4) If f is injective and g injective, is $g \circ f$ necessarily injective?

Solution.

(1) Suppose f is not injective, then there exist $a_1, a_2 \in A$ with $f(a_1) = f(a_2)$. It follows that $g(f(a_1)) = g(f(a_2))$ which implies $g \circ f$ is not injective. Therefore f is necessarily injective.

However, g is not necessarily injective: the thinking here is that maybe $g(b_1) = g(b_2)$ for some $b_1, b_2 \in B$, but one of the two elements does not get mapped by f. Then we are safe. Example:

$$\begin{cases} f : \{0,1\} \to \{0,1,2\} \\ g : \{0,1,2\} \to \{0,1\} \end{cases} \text{ with } \begin{cases} f(0) = 0 \\ f(1) = 1 \end{cases} \text{ and } \begin{cases} g(0) = 0 \\ g(1) = 1 \\ g(2) = 1 \end{cases} \text{. Then } \begin{cases} g(f(0)) = 0 \\ g(f(1)) = 1 \end{cases}$$

(2) Suppose g is not surjective, then there exists some $a^* \in A$ such that no $b \in B$ satisfy $g(b) = a^*$. Therefore there exists no $a \in A$ satisfying $g(f(a)) = a^*$, which means $g \circ f$ is not surjective. Hence g must be surjective.

However, f need not be surjective: the thinking here is that maybe some elements of B don't get mapped to by f, but if $|B| > |A|$ it's still possible that each element of B gets mapper to by g. The same example above applies to this part as well.

(3) Neither is necessarily true. Consider the following:

$$\begin{cases} f : \{0,1\} \to \{0,1,2\} \\ g : \{0,1,2\} \to \{0,1\} \end{cases} \text{ with } \begin{cases} f(0) = 1 \\ f(1) = 2 \end{cases} \text{ and } \begin{cases} g(0) = 0 \\ g(1) = 1 \\ g(2) = 1 \end{cases} \text{ .Then } \begin{cases} g(f(0)) = 1 \\ g(f(1)) = 1 \end{cases}$$

f is injective, g surjective, but $g \circ f$ neither injective nor surjective.

(4) YES. By the contrapositive of injectivity of g, if $g(f(a_1)) \neq g(f(a_2))$ then $f(a_1) \neq f(a_2)$. Then by the injectivity of f, the result becomes $a_1 \neq a_2$. Hence $g(f(a_1)) \neq g(f(a_2)) \implies a_1 \neq a_2$, so $g \circ f$ is injective.

Before moving forward, I'd like to list all the lemmas that would be helpful for this problem set. Most of them come directly from Pugh's book.

Lemma 1. Each infinite set $\mathcal{S}$ contains a denumerable subset. (Pugh 1.12)

Lemma 2. The denumerable union of denumerable sets is denumerable. (Pugh 1.18)

Lemma 3. For $m \in \mathbb{N}$, $\mathbb{Q}^m$ and $\mathbb{N}^m$ are denumerable. (Pugh 1.15, 1.20)

Lemma 4. For $m \in \mathbb{N}$, $\mathbb{Z}^m$ is denumerable.

Proof. Immediate from lemma 3 and the fact that $\mathbb{Z} \sim \mathbb{N} \sim \mathbb{Q}$. □

Lemma 5. If $\mathcal{S}$ is countably infinite, $\mathcal{T}$ is finite, and they are disjoint (for convenience), then $\mathcal{S} \sim \mathcal{S} \sqcup \mathcal{T}$.

Proof. Since $\mathcal{S}$ is countably finite, there exists bijection $f : \mathbb{N} \to \mathcal{S}$. Also, since $\mathcal{T}$ is finite, there exists bijection $g : \{1, 2, \dots, |\mathcal{T}|\} \to \mathcal{T}$. Then the function $h : \mathbb{N} \to \mathcal{S} \sqcup \mathcal{T}$ defined by

$$h(k) = \begin{cases} g(k), \text{ for } k \leqslant |\mathcal{T}| \\ f(k + |\mathcal{T}|), \text{ for } k > |\mathcal{T}| \end{cases}$$

is a bijection from $\mathbb{N}$ onto $\mathcal{S} \sqcup \mathcal{T}$. Hence $\mathcal{S} \sim \mathbb{N} \sim \mathcal{S} \sqcup \mathcal{T}$. □

Lemma 6. If disjoint $\mathcal{S}, \mathcal{T}$ are both countably infinite, then so is $\mathcal{S} \sqcup \mathcal{T}$.

Proof. Since $\mathcal{S}, \mathcal{T}$ are both countably infinite, there exist bijections $f : \mathbb{N} \to \mathcal{S}$ and $g : \mathbb{N} \to \mathcal{T}$. If we define $h : \mathbb{N} \to \mathcal{S} \cup \mathcal{T}$ by

$$h(x) = \begin{cases} f(\frac{x+1}{2}) \text{ if } x \text{ is odd} \\ g(\frac{x}{2}) \text{ if } x \text{ is even} \end{cases}$$

then the h is bijective with image $\{f(1), g(1), f(2), g(2), \dots\} = \{f(1), f(2), \dots\} \cup \{g(1), g(2), \dots\} = \mathcal{S} \cup \mathcal{T}$. □

Remark. This lemma can be generalized to the union of countable union of countably infinite sets. If it's a finite union then induction applies. If it's a countably infinite union then it's equivalent to a subset of $\mathbb{N} \times \mathbb{N}$.

Lemma 7. If $A \subset B$ with A countably infinite and B uncountable, then $B \setminus A$ is still uncountable.

Proof. The contrapositive is obvious: suppose $B \setminus A$ is countably infinite, then by lemma 6 we have $(B \setminus A) \cup A = B$ is countably infinite. □

Remark. A stronger statement for lemma 7: $|A| = |A \setminus B|$.

Problem 2. Let A be any infinite set and B be any countable set. Prove that $A \sim A \cup B$.

Solution. Since the question did not explicitly state that A and B are disjoint, it's possible that they are not. We can address this issue by defining $B' = B \setminus A$. Then A and B' are disjoint and their union $A \sqcup B' = A \cup B$. Therefore to show $A \sim A \cup B$ it suffices to show $A \sim A \sqcup B'$.

(1) If B is denumerable, then by lemma 1 we may find and construct $\mathcal{S} \subset A$, also a denumerable set. Then by lemma 6, $\mathcal{S} \cup B'$ is also denumerable. Therefore there exists a bijection $f : \mathcal{S} \cup B' \to \mathcal{S}$. If we extend the domain of f by $A \setminus \mathcal{S}$ (to make $A \cup B'$ the new domain) and define $f(x) = x$ for all $x \in A \setminus \mathcal{S}$, then we have constructed a bijection from $A \cup B'$ onto A. Hence $A \sqcup B' = A \cup B \sim A$.

(2) The proof when B is finite is analogous. Again we can find denumerable $\mathcal{S} \subset A$ and construct a bijection $g : \mathcal{S} \cup B' \to \mathcal{S}$ by lemma 5.After extending the domain we again have $A \sqcup B' \sim A \cup B \sim A$.

Problem 3 (1.38)**.** Let $\mathcal{S}$ be a set and let $\mathcal{P} = \mathcal{P}(\mathcal{S})$ be the collection of all subsets of $\mathcal{S}$. [$\mathcal{P}(\mathcal{S})$ is called the **power set** of $\mathcal{S}$.] Let $\mathcal{F}$ be the set of functions $f : \mathcal{S} \to \{0, 1\}$.

(1) Prove that there is a natural bijection from $\mathcal{F}$ onto $\mathcal{P}$ by

$$f \mapsto \{s \in \mathcal{S} : f(s) = 1\}.$$

(2) (Extra credit) prove that the cardinality of $\mathcal{P}$ is greater than that of $\mathcal{S}$, even when $\mathcal{S}$ is empty or finite.

Solution.

(1) It's easy to see that the set of all f's constitute $\mathcal{F}$. On the other hand, the set of all sets of form $\{s \in \mathcal{S} : f(s) = 1\}$ constitute $\mathcal{P}(\mathcal{S})$ because the $\mathcal{P}(\mathcal{S})$ is the collection of all subsets of $\mathcal{S}$. We can think of the value of $f_1(s)$ as a criterion on whether to "pick" or not "pick" that s as an element of a specific subset corresponding to that function f_1.

To show the mapping is bijective, we need to show it's both injective and surjective.

For injectivity, we look at the contrapositive. Suppose $\mathcal{S}_1 \subset \mathcal{S}$ is the image of both f_1 and f_2. It follows that both functions map all elements of S_1 to 1 and, since the image is $\{0, 1\}$, they both map all elements of $S \setminus \mathcal{S}_1$ to 0. Since f_1, f_2 have the same domain ($\mathcal{F}$) and codomain ($\mathcal{P}(\mathcal{S})$) and $f_1(s) = f_2(s)$ for all $s \in \mathcal{S}$, it follows that $f_1 = f_2$. Hence the mapping is injective.

Now, for surjectivity, consider any $\mathcal{S}_2 \subset \mathcal{S}$. We can always define a function $f^* : \mathcal{S} \to \{0, 1\}$ as

$$f^*(s) = \begin{cases} 1 \text{ if } s \in \mathcal{S}_2 \\ 0 \text{ otherwise} \end{cases}.$$

It becomes clear that, based on its domain and codomain, $f^* \in \mathcal{F}$. Equally clear is that, under our mapping of interest, f^* gets mapped to $\mathcal{S}_2$. Hence this mapping is both injective and bijective and is therefore bijective.

(2) Suppose $\mathcal{S}$ and $\mathcal{P}(\mathcal{S})$ have equal cardinality, then there must exist a bijection between the sets. Of course a bijection is also a surjection. We will show that there is no surjective function from $\mathcal{S}$ onto $\mathcal{P}(\mathcal{S})$.

Suppose, by contradiction, that there exists a surjection $f : \mathcal{S} \to \mathcal{P}(\mathcal{S})$. Consider the set $X = \{s \in \mathcal{S} : s \notin f(s)\}$. Clearly this is a subset of $\mathcal{S}$, so it is an element of $\mathcal{P}(\mathcal{S})$. By assumption on surjectivity, there exists $y \in \mathcal{S}$ satisfying $f(y) = X$. Where can y be?

(1) If $y \in X$, then by the definition of X we have $y \notin f(y) = X$. Contradiction.

(2) If $y \notin X$, then by the definition of X we have $f(y) \in X$. Another contradiction.

Therefore there is no place for y, i.e., $X \in \mathcal{P}(\mathcal{S})$ does *not* have a pre-image. Hence f cannot be surjective, and the cardinality of $\mathcal{P}(\mathcal{S})$ is greater than that of $\mathcal{S}$. □

Problem 4 (1.39)**.** A real number is **algebraic** if it is a root of a nonconstant polynomial with integer coefficients.

(1) Prove that the set A of algebraic numbers is denumerable.

(2) Repeat the exercise for roots of polynomials whose coefficients belong to some fixed, arbitrary denumerable set $\mathcal{S} \subset \mathbb{R}$.

(3) Repeat the exercise for roots of trigonometric polynomials with integer coefficients.

(4) Real numbers that are not algebraic are said to be **transcendental**. Trying to find transcendental numbers is said to be like looking for hay in a haystack. Why?

Solution.

(1) First we look at the cardinality of sets of polynomials of different degrees. Let A_n denote the set of all polynomials of degree $\leqslant n$ with integer coefficients. A_1 is countable in the sense that

$$A_1 \sim (\mathbb{Z} \setminus \{0\}) \times \mathbb{Z} \sim \mathbb{Z}^2 \sim \mathbb{N}^2 \sim \mathbb{N}$$

because all degree 1 polynomials with integer coefficients have the form $ax + b$ where $a \in \mathbb{Z} \setminus \{0\}$ and $b \in \mathbb{Z}$. The rest of the equivalence chain simply uses lemma 4 and the fact that $\mathbb{Z} \sim \mathbb{N}$.

For A_2, observe that

$$A_2 \sim (\mathbb{Z} \setminus \{0\}) \times \mathbb{Z}^2 \sim \mathbb{Z}^3 \sim \mathbb{N}^3 \sim \mathbb{N}$$

because all quadratic polynomials have the form $ax^2 + bx + c$ where $a \in \mathbb{Z} \setminus \{0\}$ and $b, c \in \mathbb{Z}$.

It follows that, for a degree n polynomial with integer coefficients, the only restriction is that the coefficient corresponding to the degree n term needs to be nonzero. Hence

$$A_n \sim (\mathbb{Z} \setminus \{0\}) \times \mathbb{Z}^n \sim \mathbb{Z}^{n+1} \sim \mathbb{N}^{n+1} \sim \mathbb{N}.$$

Therefore A_n is countable for all $n \in \mathbb{N}$. In other words, the set of roots of polynomials of degree n with integer coefficients is countable. Clearly we can list these sets in the pattern $A_1, A_2, \dots$, and this shows that the set $\{A_1, A_2, \dots\}$ is also countably infinite. By lemma 2, their union, the set A of roots of all nonconstant polynomials with integer coefficients, is also countably infinite / denumerable.

(2) Highly analogous to the previous part. The bulk of the proof relies on the chain $A_m \sim \mathcal{S}^{m+1} \sim \mathbb{N}^{m+1} \sim \mathbb{N}$.

(3) !

(4) By lemma 8, removing all algebraic numbers from the real, we still have an uncountable set $\mathbb{R} \setminus A$: the set of transcendental numbers. Sine the set of transcendental numbers is uncountable and the set A of algebraic numbers is countable, we know that there are "much more" transcendental numbers than algebraic numbers.

Problem 5 (1.40)**.** A **finite word** is a finite string of letters, say from the Roman alphabet.

(1) What is the cardinality of the set of all finite words, and thus of the set of all possible poems and mathematical proofs?

(2) What if the alphabet had only two letters?

(3) What if it had countably many letters?

(4) Prove that the cardinality of the set $\sum_n$ of all infinite words formed using a finite alphabet of n letters, $n \geqslant 2$, is equal to the cardinality of $\mathbb{R}$.

(5) Give a solution to Ex. 37 by justifying the equivalence chain

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} \sim \Sigma_2 \times \Sigma_2 \sim \Sigma_4 \sim \mathbb{R}.$$

(6) How many decimal expansions terminate in an infinite string of 9's? How many don't?

Solution. First note that, since finite words have finite length, there exists $n \in \mathbb{N}$ such that all finite words have lengths $\leqslant n$. (Set of lengths is nonempty and bounded above and hence has a L.U.B.)

(0) **This is what I was originally thinking about. I will call this part (0) because my actual solution for part (1) is below.** Similar to the previous proof on the cardinality of the set of algebraic numbers, here we let W_n denote the cardinality of the set of words with lengths n. Then the set of one-letter words contains 26 elements, i.e., $|W_1| = 26$. The set of two-letter words contains 26^2 elements, i.e., $|W_2| = 26^2$. The set of

k-letter words contains 26^k words, i.e., $|W_k| = 26^k$. Since we are talking about finite words, we can find $n \in \mathbb{N}$ such that n is an upper bound for all word lengths. It follows that any string of letters with length $\leqslant n$ can be a finite word. Hence the cardinality of the set $\mathcal{W}$ of all finite words is defined by

$$|\mathcal{W}| = \sum_{i=1}^{n} |W_i| = 1 + 26 + \cdots + 26^n = \frac{26^{n+1} - 1}{25}.$$

If poems and mathematical proofs are believed to be finitely long, then there exists $m \in \mathbb{N}$ such that all poems and mathematical proofs have word counts $\leqslant m$. Then the set $\mathcal{S}$ of all poems and mathematical proofs is a proper subset of the set of all "literature" with word counts $\leqslant m$ (since not all combinations of words generate poems or mathematical proofs). This set is finite with cardinality $|\mathcal{W}|^m$, and so $|\mathcal{S}| < |\mathcal{W}|^m$.

Suppose poems and proofs need not to have finite length. Then this question becomes analogous to the fourth part. See $\sum_n$ below.

(1) Note that there exists a bijection from $\mathbb{N}$ onto the set of all words created from Roman letters. Consider the following list of words / strings of letters

$$\mathbf{0}(\text{a word of zero length}), a, b, \ldots, z, aa, ab, \ldots, az, ba, \ldots, zz, aaa, aab, \ldots, zzz, aaab, \ldots$$

In this list, we first list all "words" that consists simply of one letter in lexicographical order, then all "words" consisting of two letters in lexicographical order, and so on. It becomes clear that each "word" appears precisely once. Then we can define $f(n)$ to be the n^{th} term that appears on this list.

For poems and mathematical proofs, I assume that there is a certain word limit — a proof or poem can be thousands of pages long like *Paradise Lost*, but it cannot be infinitely long. Furthermore, there must exist some $n \in \mathbb{N}$ such that *all* proofs and poems have $\leqslant n$ words. Then the cardinality of the set of all poems and proofs is $|\mathbb{N}^m|$ since we can treat each proof or poem as an m-tuple of "words". This in turn equals $|\mathbb{N}| = \aleph_0$.

(2) If the alphabet had only two letters then the answers remain the same since the list

$$\mathbf{0}, 0, 1, 00, 01, 10, 11, 000, 001, \ldots, 111, 0000, \ldots$$

is also in bijection with $\mathbb{N}$.

(3) Let A_n denote the set of all words with lengths n constructed from an alphabet with countably infinite letters. Clearly $A_1 \sim \mathbb{N}$. It's also clear that $A_2 \sim A_1 \times A_1 \sim \mathbb{N} \times \mathbb{N} \sim \mathbb{N}$. Now assume A_k is denumerable, then A_{k+1} is also denumerable in the sense that $A_{k+1} = A_k \times A_1 \sim \mathbb{N} \times \mathbb{N} \sim \mathbb{N} \times \mathbb{N}$, since every word of length $k+1$ can be constructed by appending one letter at the end of a word with length k. Hence the set of *all* words with finite length is a denumerable union of denumerable sets A_i, and this is indeed denumerable by lemma 2.

(4) Showing equal cardinality requires a bijection or injections in both directions. Below is one proof, but first note that the set $\{1, 2, \ldots, n\}$ is equivalent to the finite alphabet with n letters. From now on we will abstract the alphabet and let each number between 1 and n denote one letter in such alphabet. Then, each infinitely

long word becomes an infinitely long string with each digit between 1 and n, inclusive. Denote the set of all these strings by $\mathcal{S}$.

Proof. [1] All such strings either belong to $\mathcal{S}_{n-1}$, the set of strings with an infinite string of $(n-1)$'s at the end, or $\mathcal{S}^*$, the set of strings without such string of $(n-1)$ at the end. (Think of this analogously as an infinite string of 9's in base 10.) Hence $\mathcal{S}^* \cup \mathcal{S}_{n-1} = \mathcal{S}$. From the first question of HW3 we know that there exists a bijection $f : \mathcal{S}^* \to \mathbb{R}$.

To see that $\mathcal{S}_{n-1}$ is countable, if we omit the $(n-1)$'s at the end, we get a string of finite length. Then this set is the same as the set of all words of finite length. By part a), $\mathcal{S}_{n-1} \sim \mathbb{N}$ and is denumerable. Pick another denumerable set $\mathcal{D}$ that is disjoint from $\mathbb{R}$ (we'll see why soon), then there exists a bijection $g : \mathcal{S}_{n-1} \to \mathcal{D}$.

Now consider the function $h : \mathcal{S}^* \cup \mathcal{S}_{n-1} \to \mathbb{R} \cup \mathcal{D}$ defined by

$$h(x) = \begin{cases} f(x) \text{ if } x \in \mathcal{S}^* \\ g(x) \text{ if } x \in \mathcal{S}_{n-1} \end{cases} \quad \text{(note that } \mathbb{R} \text{ and } \mathcal{D} \text{ need to be disjoint to guarantee the bijectivity of } h)$$

which is a bijection. Hence $\mathcal{S} \sim \mathbb{R} \cup \mathcal{D}$. Now by problem 2 we have $\mathbb{R} \cup \mathcal{D} \sim \mathbb{R}$. Hence $\mathcal{S} \sim \mathbb{R}$. □

(5) The first part of the chain is immediate from the result above: $\mathbb{R} \sim \Sigma_2 \implies \mathbb{R} \times \mathbb{R} \sim \Sigma_2 \sim \Sigma_2$. For the second part, consider what $\Sigma_2 \times \Sigma_2$ means: instead of choosing one letter from the alphabet for each position in the string, now we create a pair for each position in the string. Both components of the pair are from that alphabet, so each pair has $2 \cdot 2 = 4$ possibilities. Therefore the outcome is equivalent to an infinite string generated by an alphabet with 4 letters. For example, suppose the old alphabet has two letters: a and b. Then the new alphabet has four letters: aa, ab, ba, and bb. Therefore $\Sigma_2 \times \Sigma_2 \sim \Sigma_4$. The last part is again immediate from the result in the previous part. Hence

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} \sim \Sigma_2 \times \Sigma_2 \sim \Sigma_4 \sim \mathbb{R}.$$

(6) The cardinality of decimal expansions not terminating in 9's is the same as $|\mathbb{R}| = \mathfrak{c}$, whereas the cardinality of decimal expansions with an infinite string of 9's is $|\mathbb{N}| = \aleph_0$. Both have been proven above.

[1] Idea from a chat with Linfeng. I had my own solution but it involves a complicated construction of bijection. Not as elegant as this one.