More Proofs by Contradiction

CS 234

0 Introduction

This document contains examples of good proofs based on the induction activity completed in class. These are not the only ways to write good proofs.

These proofs may contain footnotes explaining different thought processes that occurred in their construction, to help show you how to think about writing proofs. Commentary may also be provided at the end about alternative approaches.

1 Proofs

Uncountability (Red)

Theorem 1. $|\mathcal{P}(\mathbb{Q})| > |\mathbb{N}|$

Proof. Suppose for the sake of contradiction that $\mathcal{P}(\mathbb{Q})$ was in fact countable. Then its elements can be completely listed out. Let Q_i be the i^{th} set of rationals in such a listing.

At the same time, the $\mathbb{Q}$ is also countable—simply list the rationals in simplest form in shortlex order.[1]. Let q_i be the i^{th} rational in this listing.

Now consider the following set S:

$$S = \{q_i \mid q_i \notin Q_i\}$$

As every element of S is rational, it must be that $S \subseteq \mathbb{Q}$, and so $S \in \mathcal{P}(\mathbb{Q})$ by the definition of powerset. This means that S must be equal to Q_k for some k. However, if $S = Q_k$, the following also holds:

$$\begin{aligned} q_k \in S &\iff q_k \in \{q_i \mid q_i \notin Q_i\} && [S\ def] \\ &\iff q_k \notin Q_k && [\in\ def] \\ &\iff q_k \notin S && [S = Q_k] \end{aligned}$$

The fact that $q_k \in S$ iff $q_k \notin S$ is contradiction. Thus the original assumption must be false and in fact $\mathcal{P}(\mathbb{Q})$ is not countable. □

You will notice that this proof never explicitly created the infinite grid that we diagonalize over. This is because the infinite grid is really part of our scratch work—we draw it out to determine what the diagonal should be. Then once we know the answer, the proof just needs to verify that answer rather than contain the work to get there.

For reference, here what the grid we would have made could have looked like, where a checkmark in the grid cell q_i, Q_j means that $q_i \in Q_j$.

	q_0	q_1	q_2	q_3	...
Q_0	✓	✗	✓	✗	
Q_1	✗	✗	✗	✗	
Q_2	✓	✓	✓	✓	
Q_3	✗	✓	✓	✓	
⋮					

Then the set S comes from going down the diagonal and flipping the membership.

[1] It might be worth mentioning why this approach works to show countability: all rationals can be written with a finite number of symbols. Once you know that everything can be represented finitely, the set is definitely countable, as witnessed by shortlex ordering.

Uncountability (Red)

Theorem 2. $|\{f \mid f : \mathbb{N} \to \mathbb{N}\}| > |\mathbb{N}|$

Proof. Suppose for the sake of contradiction that instead $\{f \mid f : \mathbb{N} \to \mathbb{N}\}$ is countable. Then its elements can be completely listed out. Let f_i be the i^{th} function in such a listing.

Now define $g(n)$ to be $f_n(n) + 1$. Clearly $g : \mathbb{N} \to \mathbb{N}$, so g must be f_k for some k. However, $g(k) = f_k(k) + 1 \neq f_k(k)$, so g cannot be f_k since they differ on input k. This is a contradiction, so it must be that the original assumption is false and $\{f \mid f : \mathbb{N} \to \mathbb{N}\}$ is in fact uncountable.

□

Once again, for reference, here is the kind of grid that we would have made in our scratch work. In this case, each row represents a function (the rows are always those things that we are listing out), and each column represents an input. The grid cells are then the outputs.

	0	1	2	3	...
f_0	2	2	2	2	
f_1	0	1	4	9	
f_2	1	2	3	4	
f_3	0	2	4	6	
$\vdots$					

Then g is defined by going down the diagonal and changing things. For this proof's choice of changing by adding 1, g starts out by mapping 0 to 3 so that it differs from f_0 on input 0, then maps 1 to 2 so that it differs from f_1 on input 1, then maps 2 to 4 so that it differs from f_2 on input 2, then maps 3 to 7 so that it differs from f_3 on input 3, etc.

This explanation was actually longer than the proof itself! Once you find the answer, it is typically quite elegant to simply verify the answer in your proof. This is one reason to separate scratch work from the actual proof.

Non-Regularity (Green)

Theorem 3. *$\{a^p b^q c^r \mid p + q \geq r\}$ is not regular*

Proof. Let $L = \{a^p b^q c^r \mid p + q \geq r\}$. Suppose for the sake of contradiction that L is regular. Then there exists some number $k > 0$ such that all strings in L of length at leask k can be pumped.

Consider the string $a^k b^0 c^k$. Since $k + 0 \geq k$, this string is in L. Since its length is $2k \geq k$, it can also be pumped. Thus, $a^k b^0 c^k = xyz$ for some strings x, y, z where $|y| > 0$ and $|xy| \leq k$ such that, for all $i \in \mathbb{N}$, the string $xy^i z$ is also in L.

Because $|xy| \leq k$ and the first k symbols in $a^k b^0 c^k$ are all a, it must be that y is made up entirely of as. Pumping the string down therefore yields the string $a^{k-|y|} b^0 c^k$, which is guaranteed by the pumping lemma to be in L. However, $k - |y| + 0 \not\geq k$ since $|y| > 0$, so the pumped string is not in L. This is a contradiction, so L cannot be regular.

□

Non-Regularity (Blue)

Theorem 4. $\{(ab)^n(ba)^n \mid n \in \mathbb{N}\}$ *is not regular*

Proof. Let $L = \{(ab)^n(ba)^n \mid n \in \mathbb{N}\}$. Suppose for the sake of contradiction that L is regular. Then there exists some number $k > 0$ such that all strings in L of length at least k can be pumped.

Consider the string $(ab)^k(ba)^k$. This string is in L and has length $2k \geq k$, so it can be pumped. Thus $(ab)^k(ba)^k = xyz$ for some strings x, y, z where $|y| > 0$ and $|xy| \leq k$ such that, for all $i \in \mathbb{N}$, the string xy^iz is also in L.

Because $|xy| \leq k$, the string y must be some substring of the first k characters $(ab)^k$. There are then a couple of cases to consider depending on the form of y:[2]

Case $(ab)^ja$ **or** $(ba)^jb$ If $y = (ab)^ja$ or $(ba)^jb$ for some j, then the length of y is odd. Pumping the string once therefore yields a new string in L of length $2k + |y|$, which is also odd. However, every string in L is of even length, so this case leads to a contradiction.

Case $(ab)^j$ **or** $(ba)^j$ If $y = (ab)^j$ or $(ba)^j$ for some j, then $j > 0$ because $|y| > 0$. It then follows that y begins and ends with different characters, so pumping does not break the alternating pattern of as and bs in the first half of the string. Pumping the string once therefore yields the new string $(ab)^{k+j}(ba)^k$,[3] which is guaranteed to be in L by the pumping lemma. However, because $j > 0$, it must be that $k + j \neq k$ and the string's pair of adjacent bs cannot be in the middle. Thus the string cannot be in L and this case leads to a contradiction.

Because all cases lead to a contradiction, the original assumption must be false and L is in fact not regular.

□

[2] If it is not clear how these are the cases for y, try picking out different substrings of $(ab)^3$ and seeing if you can find something that does not fit these forms. You can even prove it is impossible by induction!

[3] If might not be clear how pumping $y = (ba)^j$ makes this true since $ba \neq ab$. However knowing just the length and alternation of characters is enough to determine the entire string, and we know both in this case. We can also see that this works from inspecting the pumping of $x = a, y = baba, z = bbababa$; pumping once yields $xy^2z = abababababbababa = (ab)^5(ba)^3$.