Math 79SI Notes

Mason Rogers

4 Proof by Contradiction

4.1 Background

Last week, we introduced the technique of proof by contrapositive, where to prove an implication we assume that its conclusion is false and show that at least one of its hypotheses must fail. A similar technique is proof by contradiction. As in proof by contrapositive, we begin by assuming that the conclusion is false. But instead of directly showing that one of the hypotheses fails, we invoke the hypotheses at some point in the argument and show that an absurdity is reached.

For a quick example, for real numbers x and y, consider the statement that 'if $x + y$ is irrational then x is irrational or y is irrational'. We can prove this quickly by contrapositive: suppose that x and y are rational, and it follows that $x + y$ is rational. A related statement that we would instead prove by contradiction is given by 'if x is rational and y is irrational then $x + y$ is irrational'. Assuming $x + y$ is rational does not immediately yield that x is irrational or that y is rational, as we could have x and y both rational or both irrational and still have $x + y$ be rational. Consider, for instance, $(x, y) = (0, 0)$ or $(x, y) = (\sqrt{2}, 1 - \sqrt{2})$. However, invoking the additional assumption that x is rational, we have that $x + y - x = y$ must be rational, which contradicts our other hypothesis. Thus, if x is rational and y is irrational, $x + y$ must be irrational.

To compare and contrast proof by contradiction with our other two primary techniques of proof, we consider how to prove an implication $P \implies Q$. To prove it directly, we assume P and show that Q must hold. To prove it by contrapositive, we assume Q fails and show that P must fail. To prove it by contradiction, we assume *both* that P holds and that Q fails, then show that something else goes wrong.

Occasionally, you may see arguments presented as proofs by contradiction even when they might be more accurately described as one of the other techniques. For instance, we proved that there are infinitely many prime numbers by taking an arbitrary finite list of primes L_k and constructing a prime not on that list. We could have framed the proof as a proof by contradiction by beginning with the statement 'suppose for the purpose of contradiction that there are finitely many primes and let L_k be a list of all of them', then proceeding with the same argument to "contradict" the assumption that there are only finitely many primes. However, we never meaningfully invoke the assumption that L_k is a list of *all* primes, so the argument is best left as a proof by construction. Whenever you have completed a proof by contradiction, it is a good idea to check that you have not framed it as such unnecessarily. Doing so can cloud the key elements of your argument.

As a final word on proof by contradiction, it is worth considering the relative merit of the technique compared to other techniques. Often, direct proofs or proofs by contrapositive (which we showed are equivalent using a proof by contradiction) read as a chain of reasoning in which every step provides intuition as to why the next step is true. This is often *not* the case with proofs by contradiction, for instead of aiming at the conclusion and watching it come gradually into focus, we aim for something absurd and watch the conclusion fall out. Sometimes this makes the proof less enlightening than other types of proof. However, there are many ways to evaluate the utility of proofs, and there are many circumstances in which a proof by contradiction is either the only option or the best option available. Now that we are familiar with several techniques, we will look at evaluating comparative merits of different proofs of the same statement in the activity at the end of this section.

Before diving into the examples, we introduce the notion of the *cardinality* of a set. Loosely, the cardinality of a set S, denoted $|S|$ is the size of S. For finite[1] sets, $|S|$ is simply the number of elements in the set.

We will not study the general definition of cardinality for infinite sets, but will simply define that sets A and B have the same cardinality when there exists a bijective function $f : A \to B$. For infinite sets, we will use this criterion to distinguish *countable* sets from *uncountable* sets. A countable set is any set in bijection with $\mathbb{N}$, and an uncountable set is an infinite set S such that there does *not* exist a bijective function $f : S \to \mathbb{N}$. We will omit (and in some cases relegate to future exercises) proofs of several properties that we would want our definition of cardinality to have for now. But it is worth recognizing some of the things we would want to assure ourselves that our definition captures:

- The cardinality of a finite set is a well-defined natural number.
- Every subset of a finite set is finite.
- Finite sets are in bijection if and only if they have the same cardinality.
- Any infinite subset of a countable set is countable.
- Any infinite set contains a countable infinite subset.
- If S has an uncountable subset then S is uncountable.

You may attempt to prove some of these properties now if you are interested, but we will assume them for the purpose of providing some interesting examples now.

4.2 Examples

We begin with the canonical example of a proof by contradiction: proving that $\sqrt{2}$ is irrational. Note that we proved this one way already in Corollary 2.7, in which we applied the rational root theorem to determine that the polynomial $x^2 - 2$ has no rational roots. However, use of the rational root theorem is more than what is necessary to prove the same result.

[1] We say that a set is *finite* if it is in bijection with $\{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$. Can you see how this matches our intuition for a set having finitely many elements?

Proposition 4.1. $\sqrt{2}$ is irrational.

Proof. We rephrase the statement to make it more clear how we will use proof by contradiction. Consider the statement 'if x is a real number such that $x^2 = 2$ then x is irrational'.[2] It is now clear that the hypothesis is 'x is a real number such that $x^2 = 2$' and that the conclusion is 'x is irrational'. For our proof by contradiction, we assume both that x is rational (i.e. that our conclusion is false) and that $x^2 = 2$ (i.e. that our hypothesis is true).

Since x is rational, we can write x *in lowest terms* as $\frac{a}{b}$. (The assumption of x being expressed in lowest terms is key, as it will be what we ultimately contradict.) Accordingly, $x^2 = \frac{a^2}{b^2}$, which by assumption equals 2. Multiplying through by b^2 reveals that

$$a^2 = 2b^2, \tag{1}$$

and in particular that a^2 is even. We proved in Proposition 3.3 of the previous section that a^2 being even implies that a is even. If we can show that b must also be even, then since $a, b \neq 0$, $\frac{a}{b}$ would not be in lowest terms, yielding the desired contradiction. To do this, we will leverage the fact that even squares are necessarily divisible by 4.

Because a is even, write $a = 2k$ for some integer k. Returning to equation (1) and substituting $a = 2k$ yields $4k^2 = 2b^2$, or more simply that $b^2 = 2k^2$. Thus, b^2 is even, and by Proposition 3.3, b is even.

We have achieved a contradiction, since if a and b are both even and nonzero, $\frac{a}{b}$ is not in lowest terms as assumed. This concludes the proof. □

Let us recap our argument. We began by assuming that the conclusion 'x is irrational' was false, but instead of showing that the assumption '$x^2 = 2$' must have been false, we additionally assumed that $x^2 = 2$ and showed that something impossible resulted. Thus, our assumptions were incompatible, and the desired statement followed.

Such an argument could also be worded more succinctly by beginning with the phrase 'suppose for the purpose of contradiction that $\sqrt{2}$ is rational, i.e. that $\sqrt{2} = \frac{a}{b}$, where $\frac{a}{b}$ is in lowest terms' and proceeding as we did. We chose to write the expanded argument to emphasize the *technique*; however, as the technique becomes familiar to you, it is better to emphasize the *argument*.

We can sometimes use proof by contradiction to establish that certain equations do not have solutions that meet specified conditions. We will consider two examples of *Diophantine equations*, or polynomial equations in integer unknowns, which do not admit solutions.

Proposition 4.2. The equation $x^2 - y^2 = 10$ does not have any solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

Proof. Suppose for the purpose of contradiction that such a solution (x, y) exists. Then we have $x^2 - y^2 = (x - y)(x + y) = 10$, where $x + y$ and $x - y$ are integers. The only factorizations of 10 into two factors are $10 \cdot 1, 5 \cdot 2, 2 \cdot 5$, and $1 \cdot 10$. In all four cases, the factors have opposite parity; however, $x + y$ and $x - y$ have the same parity. Thus, we have achieved a contradiction, and there are no integer solutions to $x^2 - y^2 = 10$. □

In this case, we actually contradicted the existence of the solution of the equation. For the next equation, we will have to use a craftier argument to contradict a supposed *property* of the solution.

[2]Note that this will prove the slightly more general statement that $\sqrt{2}$ and $-\sqrt{2}$ are irrational.

Proposition 4.3. The only integer solution to $x^2 + y^2 = 3z^2$ is $(x, y, z) = (0, 0, 0)$.

Proof. Suppose for the purpose of contradiction that there exists a solution (x', y', z') other than $(0, 0, 0)$. Then dividing by the greatest common divisor of x', y', and z',[3] we can choose a new solution (x, y, z) such that the greatest common divisor of x, y, and z is 1, and in particular not all of x, y, and z are even.

From the argument in the claim within Proposition 3.6, z^2 leaves remainder 0 or 1 after dividing by 4. Consequently, $3z^2$ leaves remainder 0 or 3 after dividing by 4. However, since $3z^2$ is the sum of two squares, Proposition 3.6 rules out the case that $3z^2$ leaves remainder 3 after dividing by 4. In other words, $3z^2$ is a multiple of 4, and in particular $3z^2$ is even. Because 3 is odd, we know that z^2 must be even, and by Proposition 3.3 we see that z is even.

Stepping back a few sentences, recall that $3z^2$ leaves remainder 0 after dividing by 4. Again by the claim in Proposition 3.6, x^2 and y^2 leave remainder 0 or 1 after dividing by 4. The only way for $x^2 + y^2$ to leave remainder 0 after dividing by 4 is for x^2 and y^2 each to leave remainder 0 after dividing by 4. Again, it follows that x^2 and y^2 are even, then that x and y are even. We conclude that x, y, and z must all be even. This contradicts the assumption that the greatest common divisor of x, y, and z is 1, so we conclude that (x, y, z) cannot exist as prescribed. Thus, there are no integer solutions to $x^2 + y^2 = 3z^2$ other than $(0, 0, 0)$. □

Another argument by contradiction yields the following corollary:

Corollary 4.4. The curve in the uv-plane generated by $u^2 + v^2 = 3$ contains no rational points.

Proof. Suppose for the purpose of contradiction that there exist rational numbers u and v such that $u^2 + v^2 = 3$. Let $u = \frac{a}{b}$ and $v = \frac{c}{d}$, where both fractions are in lowest terms. Substituting gives

$$\left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2 = 3,$$

and multiplying through by b^2d^2 gives $(ad)^2 + (bc)^2 = 3(bd)^2$ for some integers a, b, c, and d.

As proven above, however, this is only possible if $ad = 0, bc = 0$, and $bd = 0$. Note that b and d are nonzero since they are the denominators of fractions, so necessarily $a = c = 0$. Hence, $u = v = 0$, which is not a solution to $u^2 + v^2 = 3$. Thus, we have achieved a contradiction, and $u^2 + v^2 = 3$ has no rational points. □

4.3 Exercises

1. Prove that there are infinitely many prime numbers p such that $p + 2$ is composite.

2. In this problem we will prove a few results about countable sets. Let A_i be a countable set for all $i \in \mathbb{N}$.

   (a) Prove that the union $A_1 \cup A_2$ is countable.

[3] We define the greatest common divisor of 3 numbers to be the largest positive integer which is a divisor of all 3.

(b) Prove that the union $\cup_{i\in\mathbb{N}} A_i$ is countable. (*Hint: Try to apply a similar technique to the one used in proving the countability of* $\mathbb{Q}$.)

(c) Prove that the Cartesian product $A_1 \times A_2$ is countable.

(d) Find an example of a countable collection of finite sets B_i such that $\times_{i\in\mathbb{N}} B_i := B_1 \times B_2 \times \cdots$ is *not* countable.[4] (*Hint: Think about decimal expansions.*)

3. Determine whether the following sets are finite, countable, or uncountable. (You may use the unproven properties of cardinality suggested in section 4.1.)

(a) The set of prime numbers

(b) $\mathbb{C}$

(c) The set of *Gaussian integers*, i.e. complex numbers $a + bi$ where $a, b \in \mathbb{Z}$

(d) The set of *algebraic numbers*, i.e. roots of polynomials with integer coefficients

Additionally, prove that *transcendental numbers*, i.e. complex numbers which are not algebraic, exist. (*Note: Even though this proves that transcendental numbers exist, it does not provide any examples or even hints at what examples might look like.*)

4. Determine exactly for which integers c the equation $x^2 - y^2 = c$ admits integer solutions. Prove your answer. You may use the fundamental theorem of arithmetic in your proof if needed. (*Hint: Start by proving that for integers a and b, there exist integers x and y such that $x + y = a$ and $x - y = b$ if and only if a and b have the same parity.*)

5. A polynomial with integer coefficients is called *primitive* if the greatest common divisor of all of its coefficients is 1. Prove that if f and g are primitive, fg is also primitive. You may use Euclid's lemma, which states that if a prime p divides the product ab, either $p \mid a$ or $p \mid b$. (*Hint: Assuming f and g are primitive, for any prime p you can chose the highest-degree term of f and g such that the corresponding coefficient is not divisible by p.*)

6. Using the previous exercise, prove that if h is a primitive polynomial that cannot be written as a product fg of non-constant integer-coefficient polynomials f and g, h cannot be written as a product pq of non-constant rational-coefficient polynomials p and q either. This result is known as Gauss's Lemma. (*Hint: Suppose p and q exist, then clear denominators.*)

7. We will prove some lower bounds for the Hadwiger-Nelson problem, which asks for the smallest number n of colors needed to paint every point in the plane such that no 2 points at distance 1 from each other have the same color. (*Hint: Think about triangles.*)

(a) Prove that $n > 2$.

(b) Prove that $n > 3$.

[4] The notation := indicates that we are defining the object on the left to equal the object on the right. It is also common to flip the notation and write =: to make the definition the other way.

It is known that $5 \leq n \leq 7$. The upper bound of 7 is given by a certain coloring of a hexagonal tesselation of the plane. The lower bound of 5 can be proven by similar techniques to those used for this problem.

8. You may find it surprising to learn that the number line $\mathbb{R}$ and the coordinate plane $\mathbb{R} \times \mathbb{R}$ have the same cardinality. (In fact, the same is true for any infinite set S and $S \times S$.) Google 'Peano curve' and write a few things that you learn. Do you think there exists a differentiable construction of a space filling curve? The answer follows from Sard's theorem, a fundamental result in differential topology.

4.4 Further Reading

CPZ Chapter 5.2, 5.5	Discussion of proof by contradiction.
"The Proof", Nova Documentary dir. Simon Singh	An interesting documentary (50 min) on the proof of Fermat's last theorem, a famously longstanding open problem in number theory answered by Andrew Wiles in 1994. http://www.dailymotion.com/video/x1btavd
Wikipedia entry for Cardinality	More on cardinality at a level of specificity greater than necessary for this section. https://en.wikipedia.org/wiki/Cardinality

4.5 Further Examples

We now move to a series of statements about cardinalities of common infinite sets, culminating in a famous proof by contradiction about the cardinality of $\mathbb{R}$. We will see that while cardinality captures some intuitions about sizes of infinite sets, it fails to match others. As such, there may be other useful notions of 'size of a set' that capture those intuitions.

Proposition 4.5. $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ are countable.

Proof. Recall that a set S is countable if it there exists a bijection between S and $\mathbb{N}$. Sometimes, the easiest way to prove the existence of a certain function is to construct it explicitly, which is exactly what we will do here.

Observe that the identity map on $\mathbb{N}$ is a bijection from $\mathbb{N}$ to itself, so $\mathbb{N}$ is trivially countable.

It is trickier to show that $\mathbb{Z}$ is countable, for $\mathbb{N}$ includes in $\mathbb{Z}$ naturally as a proper subset. However, consider the map $f : \mathbb{Z} \to \mathbb{N}$ given by sequentially enumerating integers with alternating sign, i.e. $0 \mapsto 1, 1 \mapsto 2, -1 \mapsto 3, 2 \mapsto 4, -2 \mapsto 5$, etc.[5] We want to show that f is a bijection between $\mathbb{Z}$ and $\mathbb{N}$, so we must check three things: that f is a valid function, that f is injective, and that f is surjective.

[5]The arrow '$\to$' is used to describe which sets a function maps between, while the arrow '$\mapsto$' is used to describe where the function maps particular elements. The arrow '$\hookrightarrow$' is like $\to$, but denotes that the function is injective.

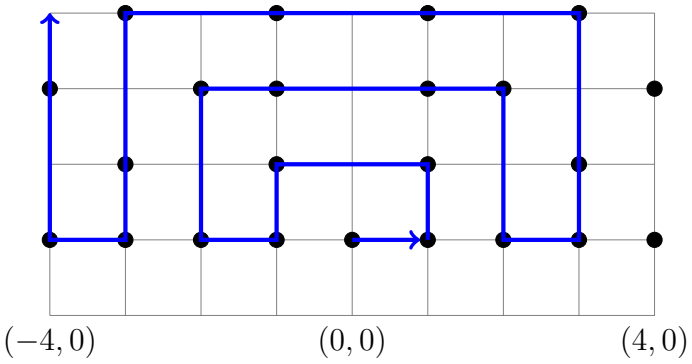

Figure 1: The black dots represent elements of $\mathbb{Q}$. If q is the n-th point hit by the depicted path, we define $f(q) = n$.

To check that f is a valid function, we must check that for every element of $\mathbb{Z}$, f assigns a unique element of $\mathbb{N}$.[6] In this case, however, we can check that f assigns an element of $\mathbb{N}$ to each element of $\mathbb{Z}$ simply by writing $f(k)$ for all $k \in \mathbb{Z}$. We have

$$f(k) = \begin{cases} 2k & k > 0 \\ -2k + 1 & k \leq 0, \end{cases}$$

and it is clear that f assigns a natural number to every integer. To see that f is injective, observe that in our procedure for defining values of f, we never let f take the same value twice, and it follows that f is injective. To see that f is surjective, observe from our formula for $f(k)$ above that the image of f contains all even and odd natural numbers. Thus, f is a well-defined bijection from $\mathbb{Z}$ to $\mathbb{N}$, and $\mathbb{Z}$ is countable.

To construct a bijection $f : \mathbb{Q} \to \mathbb{N}$, we will consider elements of $\mathbb{Q}$ to be ordered pairs $(a, b) \in \mathbb{Z} \times \mathbb{Z}$[7] where $b > 0$ and $\gcd(a, b) = 1$.[8] We then enumerate the elements of $\mathbb{Q}$ by starting at $(0, 1)$ and spiraling outward as depicted in figure 1.

As before, we must check three things: that this procedure assigns a natural number to every rational number, that the assignment is injective, and that it is surjective.

While it is difficult to write an explicit formula for f, we can show that $f(q)$ is well defined by bounding it above to observe that indeed every rational number is assigned a finite value. For $q = \frac{a}{b}$ in lowest terms, let $M = \max\{|a|, |b|\}$, and observe that $f(q)$ is bounded above by the finite number of integer-coordinate points inside the rectangle with vertices $(-M, 0), (M, 0), (M, M), (-M, M)$. We conclude that f assigns a finite value to each $q \in \mathbb{Q}$, so f is truly a function $f : \mathbb{Q} \to \mathbb{N}$.

[6] This is necessary because if we define a function procedurally, we need to make sure that all elements of the domain are assigned values. For instance, defining g as a purported function from $\mathbb{Z}$ to $\mathbb{N}$ by $1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 3$, etc. gives an injection and a surjection; however, g is not even a function from $\mathbb{Z}$ to $\mathbb{N}$, since g never assigns values to all elements of $\mathbb{Z}$.

[7] The *Cartesian product* of two sets S and T, denoted '$S \times T$', is the set of ordered pairs (s, t) where $s \in S$ and $t \in T$. A familiar example is the coordinate plane $\mathbb{R} \times \mathbb{R}$.

[8] Implicitly, we are using the fact that any rational number can be written in lowest terms with positive denominator uniquely to construct a bijection g from $\mathbb{Q}$ to the subset of $\mathbb{Z} \times \mathbb{Z}$ with coprime coordinates and positive second coordinate.

Injectivity of f follows from the fact that each value in $\mathbb{N}$ is assigned only once, as in the $\mathbb{Z}$ case.

We prove surjectivity by showing that for an arbitrary $n \in \mathbb{N}$, there exists $q \in \mathbb{Q}$ such that $f(q) = n$. Observe that if $f(q) = n$, then all natural numbers $m < n$ have also been assigned, so there exists q' such that $f(q') = m$ for any natural number $m < n$. Additionally, observe that for natural numbers n, $f(n) > n$. Thus, for any natural number n, $f(n) > n$, and the value n must have been assigned to some other rational number q'. We conclude that f is surjective.

In sum, we have constructed a well-defined bijection from $\mathbb{Q}$ to $\mathbb{N}$, and we conclude that $\mathbb{Q}$ is countable. □

Perhaps it is surprising that even though $\mathbb{Q}$ and $\mathbb{Z}$ might seem like much larger sets than $\mathbb{N}$, we can choose one-to-one correspondences between them. You might be inclined to ask whether the same is true for $\mathbb{R}$, but this turns out not to be the case.

In proving that $\mathbb{R}$ is uncountable, we invoke the fact that any real number $x \in (0, 1)$ has a unique decimal expansion $x = .a_1a_2a_3\ldots$ such that $a_i \in \{0, 1, \ldots 9\}$ for all $i \in \mathbb{N}$ and there does *not* exist $N \in \mathbb{N}$ such that $a_i = 9$ for all $i > N$. (The condition that a_i must be something other than 9 for infinitely many i is simply to eliminate redundancy such as $.1 = .0\overline{9}$.)

Theorem 4.6. $\mathbb{R}$ is uncountable.

Proof (Cantor's Diagonal Argument). Since we are granting the fact that a superset of an uncountable set is uncountable and $\mathbb{R} \supset (0, 1)$, it suffices to prove that $(0, 1)$ is uncountable.

Suppose for the purpose of contradiction that $(0, 1)$ is countable, and choose an enumeration $n \mapsto x_n$ of the elements of $(0, 1)$. That is, choose a bijection $f : \mathbb{N} \to (0, 1)$ and define $x_n = f(n)$. As mentioned above, each x_n has a unique decimal expansion $.a_{n_1}a_{n_2}a_{n_3}\ldots$ subject to the condition of avoiding expansions like $.0\overline{9}$ and choosing .1 instead.

Consider a sequence b_i chosen such that $b_i \in \{0, 1\ldots, 9\}$ for all $i \in \mathbb{N}$, $b_i \neq a_{i_i}$ and $b_i \neq b_{i-1}$ for every $i \in \mathbb{N}$. Such a sequence necessarily possible to construct since a_{i_i} and b_{i-1} can comprise at most 2 of the 10 possibilities for b_i. Moreover, $.b_1b_2b_3\ldots$ is a decimal expansion for some real number $y \in [0, 1]$.

We now aim to show that $y \in (0, 1)$ and $y \neq x_n$ for any $n \in \mathbb{N}$. First, observe that $y \in (0, 1)$ since the only decimal expansions for 0 and 1 are $.\overline{0}$ and $.\overline{9}$ respectively, both of which are forbidden by the restriction $b_i \neq b_{i-1}$. We thus just must show that $y \neq x_n$ for any n.

By construction, the i-th digit of the decimal expansion for y (specifically b_i) does not equal the i-th digit of the decimal expansion for x_i (specifically a_{i_i}), so the chosen decimal expansion for y does not match that of any of the x_n. The only way for distinct decimal expansions to have the same value is if they differ by an exchange of form $.0\overline{9} \leftrightarrow .1$. By assumption, all of the chosen expansions a_{n_i} for the x_n have infinitely many entries not equal to 9, and by the condition that $b_i \neq b_{i-1}$, so does the expansion b_i of y. Thus, $y \neq x_n$ for all $n \in \mathbb{N}$, and we have found an element of $(0, 1)$ which is not in the image of f. This contradicts the assumption that f is surjective, so we conclude that no bijection exists between $\mathbb{N}$ and $(0, 1)$. Thus, $(0, 1)$ is uncountable, and so is $\mathbb{R}$. □

One intuition that this result solidifies is that there are "more" real numbers than rational numbers.