2: GEOMETRY, PROBABILITY, AND CARDINALITY

STEVEN HEILMAN

1. The Pythagorean Theorem

Suppose a right triangle has edges A, B, C with corresponding lengths a, b, c. Suppose C is the hypotenuse. Let θ be the angle of the triangle formed by the edges A and C. From the definitions of trigonometric functions that we used in high school, $\cos\theta = a/c$ and $\sin\theta = b/c$. Also, from an identity that we learned in high school, $(\cos\theta)^2 + (\sin\theta)^2 = 1$, so $(a/c)^2 + (b/c)^2 = 1$, i.e. $a^2 + b^2 = c^2$. However, if $a^2 + b^2 = c^2$, then we can reverse this reasoning to conclude that $(\cos\theta)^2 + (\sin\theta)^2 = 1$. So, it seems that the Pythagorean Theorem is more or less equivalent to the identity $(\cos\theta)^2 + (\sin\theta)^2 = 1$.

To avoid circular reasoning, we would like to give a proof of the Pythagorean Theorem from first principles. In some sense the first proof will be roundabout, since a simpler proof could be given. However, the concepts that we introduce are actually extremely important, though this may not be clear right now. Since the rigorous treatment of limits is not a prerequisite of this course, we will not treat limits in a rigorous fashion. Try to find where these details are avoided.

Let $x \in \mathbb{R}$. We define $\sin x$ and $\cos x$ by the following formulas.

$$\sin x = \sum_{k\geq 0} \frac{x^{2k+1}(-1)^k}{(2k+1)!}, \qquad \cos x = \sum_{k\geq 0} \frac{x^{2k}(-1)^k}{(2k)!}$$

(Recall that $0! = 1$. Also, the sum over $k \geq 0$ is shorthand for $k \geq 0, k \in \mathbb{Z}$.) Denote i as the complex number such that $i = \sqrt{-1}$. Recall that the complex numbers $\mathbb{C}$ are defined as follows

$$\mathbb{C} = \{a + bi \colon a, b \in \mathbb{R}\}$$

For a complex number $z = a+bi$ with $a, b \in \mathbb{R}$, recall that we define the complex conjugate $\overline{z}$ of z by the formula $\overline{z} = a - bi$. Recall also that we define the absolute value of a complex number z by the formula

$$|z| = \sqrt{z\overline{z}} = \sqrt{(a+bi)(a-bi)} = \sqrt{a^2+b^2}$$

We also define the exponential function via the following formula.

$$e^z = \sum_{k\geq 0} \frac{z^k}{k!}$$

Our proof of the Pythagorean Theorem will result from a series of identities that involve the exponential function and i.

Theorem 1.1. *Let $x \in \mathbb{R}$. Then*

$$e^{ix} = \cos x + i \sin x$$

Date: April 29, 2012.

Proof.

$$\begin{aligned}
e^{ix} &= \sum_{k\geq 0} \frac{(ix)^k}{k!} = \left(\sum_{k\geq 0\colon\, k \text{ even}} \frac{(ix)^k}{k!} \right) + \left(\sum_{k\geq 0\colon\, k \text{ odd}} \frac{(ix)^k}{k!} \right) \\
&= \left(\sum_{j\geq 0} \frac{(ix)^{2j}}{(2j)!} \right) + \left(\sum_{\ell\geq 0} \frac{(ix)^{2\ell+1}}{(2\ell+1)!} \right) \\
&= \left(\sum_{j\geq 0} \frac{(-1)^j x^{2j}}{(2j)!} \right) + \left(\sum_{\ell\geq 0} \frac{i(-1)^\ell (x)^{2\ell+1}}{(2\ell+1)!} \right) \\
&= \cos x + i \sin x
\end{aligned}$$

□

Corollary 1.2. *Let $x \in \mathbb{R}$. Then the complex conjugate of e^{ix} is e^{-ix}.*

Proof.

$$\overline{e^{ix}} = \overline{\cos x + i \sin x} = \cos x - i \sin x = \cos(-x) + i \sin(-x) = e^{-ix}$$

□

Corollary 1.3. *Let $x \in \mathbb{R}$. Then*

$$\cos x = \frac{e^{ix} + e^{-ix}}{2}, \qquad \sin x = \frac{e^{ix} - e^{-ix}}{2i}$$

Proof. Add and subtract the following two identities

$$e^{ix} = \cos x + i \sin x, \qquad e^{-ix} = \cos x - i \sin x$$

□

Theorem 1.4. *Let $w, z \in \mathbb{C}$. Then $e^{w+z} = e^w e^z$.*

Proof. Let $\ell \geq 0, \ell \in \mathbb{Z}$. From the binomial theorem, $(w+z)^\ell = \sum_{k=0}^{\ell} w^k z^{\ell-k} \frac{\ell!}{k!(\ell-k)!}$. Then

$$\begin{aligned}
e^w e^z &= \left(\sum_{k=0}^{\infty} \frac{w^k}{k!} \right) \left(\sum_{j=0}^{\infty} \frac{z^j}{j!} \right) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{\infty} \frac{w^k z^j}{(k!)(j!)} \right) \\
&= \sum_{\ell=0}^{\infty} \left(\sum_{j,k\geq 0\colon\, j+k=\ell} \frac{w^k z^j}{(k!)(j!)} \right) \qquad \text{, re-indexing the summation} \\
&= \sum_{\ell=0}^{\infty} \sum_{k=0}^{\ell} \frac{w^k z^{\ell-k}}{k!(\ell-k)!} \qquad \text{, re-indexing the summation} \\
&= \sum_{\ell=0}^{\infty} \frac{(w+z)^\ell}{\ell!} \qquad \text{, from the binomial theorem} \\
&= e^{w+z}
\end{aligned}$$

□

We can now finish our proof of the Pythagorean Theorem

Theorem 1.5. *For $\theta \in \mathbb{R}$, $(\cos\theta)^2 + (\sin\theta)^2 = 1$.*

Proof.

$$\begin{aligned}(\cos\theta)^2 + (\sin\theta)^2 &= |e^{i\theta}|^2 \qquad \text{, by Theorem 1.1 and the definition of absolute value}\\ &= e^{i\theta}\,\overline{e^{i\theta}} = e^{i\theta}e^{-i\theta} \qquad \text{, by Corollary 1.2}\\ &= e^{i\theta - i\theta} \qquad \text{, by Theorem 1.4}\\ &= 1\end{aligned}$$

□

Theorem 1.6. ***(Pythagorean Theorem)*** *Suppose we have a right triangle with edge lengths $a, b, c > 0$ where c is the length of the hypotenuse. Then $a^2 + b^2 = c^2$.*

Proof. For $\theta \in (0, \pi/2)$ define a point $f(\theta)$ in the plane $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ by the formula

$$f(\theta) = (\cos\theta, \sin\theta)$$

That is, $\cos\theta$ is the x-coordinate, and $\sin\theta$ is the y-coordinate. The distance in $\mathbb{R}^2$ from $f(\theta) = (\cos\theta, \sin\theta)$ to the origin $(0, 0)$ is given by $\sqrt{(\cos\theta)^2 + (\sin\theta)^2} = 1$, using Theorem 1.5. So, $f(\theta)$ lies on the unit circle, centered at the origin. Let the given right triangle be embedded in the plane $\mathbb{R}^2$ so that one of its edges lies in the x-axis $\{(x, y) \in \mathbb{R}^2 \colon y = 0\}$. Also, let the the hypotenuse lie in the upper right quadrant $\{(x, y) \in \mathbb{R}^2 \colon x \geq 0, y \geq 0\}$, so that the hypotenuse has one endpoint at the origin. By the definition of $f(\theta)$, there exists $\theta \in (0, \pi/2)$ so that $c \cdot f(\theta) = (c \cdot \cos\theta, c \cdot \sin\theta)$ is an endpoint of the hypotenuse. By the definition of $f(\theta)$ and by Theorem 1.5

$$\sqrt{a^2 + b^2} = \sqrt{(c \cdot \cos\theta)^2 + (c \cdot \sin\theta)^2} = c$$

Since $a, b, c > 0$, we conclude that $a^2 + b^2 = c^2$ □

Remark 1.7. In this proof, we used a formula for distances in the plane. In truth, this formula relies on the Pythagorean Theorem, so in some sense we may consider this proof to use circular reasoning. For this reason, and to reinforce our geometric proofs from class, we present below Euclid's original proof of the Pythagorean Theorem. We will freely use some facts from elementary geometry. As an exercise, try to find where these elementary facts are used, and perhaps even try to prove them.

Remark 1.8. In the next set of notes we some surprising applications of the exponential function. The above properties of the exponential function can be used to derive multiple angle formulas for sine and cosine. For example,

$$(\cos\theta)^2 - (\sin\theta)^2 + 2i\sin\theta\cos\theta = (\cos\theta + i\sin\theta)^2 = (e^{i\theta})^2 = e^{2i\theta} = \cos 2\theta + i\sin 2\theta$$

Equation the real and imaginary parts of this equation, we conclude that

$$\cos 2\theta = (\cos\theta)^2 - (\sin\theta)^2 \qquad \text{and} \qquad \sin 2\theta = 2\sin\theta\cos\theta$$

This process can be continued.

$$(\cos\theta)^3 - 3\cos\theta(\sin\theta)^2 + 3i\sin\theta(\cos\theta)^2 - i(\sin\theta)^3 = (e^{i\theta})^3 = e^{3i\theta} = \cos 3\theta + i\sin 3\theta$$

Therefore, $\cos 3\theta = (\cos\theta)^3 - 3\cos\theta(\sin\theta)^2$ and $\sin 3\theta = 3\sin\theta(\cos\theta)^2 - (\sin\theta)^3$.

Theorem 1.9. ***(Pythagorean Theorem)*** *Suppose we have a right triangle with edge lengths $a, b, c > 0$ where c is the length of the hypotenuse. Then $a^2 + b^2 = c^2$.*

Proof. In counter-clockwise order, label the vertices of the triangle with labels A, B, C, such that BC is the hypotenuse. When referring to planar figures, we will always refer to vertices in counter-clockwise order. On each edge of the triangle, construct a square that does not intersect the original triangle. So, on edge AC construct square $ACKH$. On edge BA construct a square $BAGF$. And on the hypotenuse CB construct a square $CBDE$. We are required to show that the area of square $ACKH$ plus the area of square $BAGF$ equals the area of square $CBDE$. Draw lines BK, FC, AD and AE. Finally, let L be a point on DE so that the segment AL is perpendicular to DE. We have the following figure.

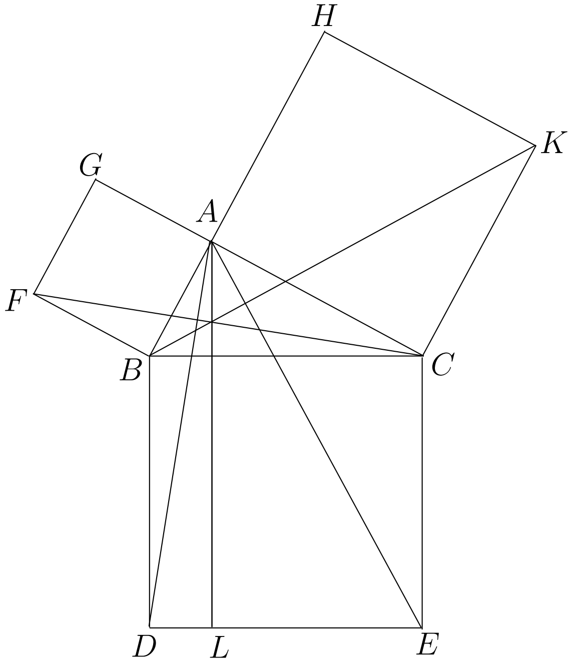

FIGURE 1. Euclid's windmill.

To prove the theorem, we will show that the rectangle with vertices B, L along its diagonal has the same area as square $BAGF$. By a similar argument, the rectangle with vertices C, L along its diagonal has the same area as square $ACHK$. Combining these two facts proves that the area of square $ACKH$ plus the area of square $BAGF$ equals the area of square $CBDE$, completing the theorem.

For an angle formed by three vertices A_1, A_2, A_3, we denote this angle by $\angle A_1A_2A_3$. We denote the measure of $\angle A_1A_2A_3$ with the notation $m\angle A_1A_2A_3$.

We prove the first fact. Note that $\angle FBA$ and $\angle CBD$ are both right angles. So,

$$m\angle FBC = m\angle FBA + m\angle ABC = m\angle CBD + m\angle ABC = m\angle ABD$$

Since $BAGF$ and $CBDE$ are squares, we conclude that edges BA and FB have the same length, and edges CB and BD have the same length. So, by the side-angle-side criterion for triangles ABD and FBC, we conclude that the area of triangle ABD is equal to the area of triangle FBC.

Observe that triangle ABD has half the area of the parallelogram with diagonal BL, since they share the segment BD, and they are both bounded by the parallel lines BD, AL. Similarly, triangle FBC has half the area of the parallelogram with diagonal AF, since they share the segment FB, and they are both bounded by the parallel lines FB, AG.

Combining these observations, we conclude that the rectangle with diagonal BL has area equal to that of square $BAGF$. By an analogous argument, the rectangle with diagonal CL has area equal to that of the square $ACKH$. Combining these facts, the area of square $ACKH$ plus the area of square $BAGF$ equals the area of square $CBDE$, as desired. □

2. An Aside: The Limit of Proofs

Within this course, we implicitly assume that: a mathematical proof is the ultimate statement of mathematical truth. However, many facts or statements from the sciences or from mathematics itself may never be expressed via a formal mathematical proof. Also, many mathematical statements are often influenced by intuitive calculations, by analogies from physics, etc. For example, consider the figure-eight trajectory of the NASA Apollo missions. This trajectory is known as the free-return trajectory, circumlunar trajectory, or lunar orbit rendezvous. In this trajectory, a spacecraft travels in a figure-eight motion by leaving the earth, circling around the moon, and then returning to the earth. In the early 1900s, physicists Yuri Kondryatuk and Hermann Oberth had explored the possibility of such a trajectory for travel to and from the moon. Around 1960, some independent research teams, one of which included Clinton Brown and William Michael, further developed this idea. Ultimately, John Houboult promoted this trajectory over other plans, and it was implemented in the Apollo missions. Perhaps this trajectory even saved the Apollo 13 mission, since it allowed the spacecraft to return to earth with a minimal expense of energy.

The investigations into this trajectory used calculations on computers and on paper. So, it took more than just mathematical proofs to achieve the goal at hand. However, rigorous thinking indeed played a great role in this endeavor. So, even though a proof of a mathematical statement is an excellent achievement, it is only one piece of a larger body of work.

3. Conditional Probability: False Positives in Medical Testing

Suppose I go to the doctor's office, I have some medical test done, and the test says that I have some disease. Do I actually have the disease? Can I quantify the certainty or uncertainty in my diagnosis?

Consider the following example. If I do not have the disease, there is a 1% chance that the test says that I do have the disease (i.e. a false positive occurs). If I do have the disease, there is a 99% chance that the test says that I do have the disease. Suppose also that this disease is rare, so that only .1% of the population has this disease.

If the test says that I have the disease, do I actually have this disease? Let us first investigate with an artificial model of the population. Suppose there are only $100,000$ people in the world. Then 100 of them have the disease, and $99,900$ of them do not. Of the 100 with the disease, the test will say that about 99 of them will have the disease. Of the $99,900$ that do not have the disease, the test will say that about 999 of them have the disease. So, among the people that test positive for the disease, only $99/(999+99)$ or about 9% actually have the disease. Even though the test seemed accurate, it turns out that it does not tell us very much.

We now turn this analysis into a theorem. Let A and B be sets in some universe. We think of the sets A, B as events that can occur in the world, so that the universal set is the set of all possible events. In the above example, I define A to be the event that I am sick with the disease, and I define B to be the event that I test positive for the disease. We are interested in the probability that A occurs, given that B has already occurred. We denote $P(A)$ as the probability that A occurs, so that $0 \leq P(A) \leq 1$. Since P denotes the probability of two events, if A and B satisfy $A \cap B = \emptyset$, then $P(A \cup B) = P(A) + P(B)$. That is, if two events are totally different, then their probabilities add.

We define

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Here $P(A|B)$ is the probability that A occurs, given that B has occurred already. In order to compute the probability $P(A|B)$, we will use the following formula.

Theorem 3.1. ***(Bayes' formula)***

$$P(A|B) = \frac{P(B|A)P(A)}{P(B|A)P(A) + P(B|A^c)P(A^c)}$$

Proof.

$$\begin{aligned}
P(A|B) &= \frac{P(A \cap B)}{P(B)} && \text{, by the definition of } P(A|B) \\
&= \frac{P(A \cap B)P(A)}{P(B)P(A)} = \frac{P(B|A)P(A)}{P(B)} && \text{, by the definition of } P(B|A) \\
&= \frac{P(B|A)P(A)}{P((B \cap A) \cup (B \cap A^c))} \\
&= \frac{P(B|A)P(A)}{P(B \cap A) + P(B \cap A^c)} && \text{, since } (B \cap A) \cap (B \cap A^c) = \emptyset \\
&= \frac{P(B|A)P(A)}{P(B|A)P(A) + P(B|A^c)P(A^c)}
\end{aligned}$$

□

We can now give a solution to our problem in medical diagnosis. Define A to be the event that I am sick with the disease, and define B to be the event that I test positive for the disease. It is given that $P(B|A) = .99$, $P(A) = .001$, $P(B|A^c) = .01$, and $P(A^c) = .99$. Therefore,

$$P(A|B) = \frac{.99(.001)}{.99(.001) + .01(.99)} = \frac{1}{11}$$

To reiterate, it turns out that this test does not tell us very much. Even if the test result is positive, there is only a 1/11 chance that I am sick with the disease. It seems that we need to create a new test that is more accurate.

Exercise 3.2. To test your understanding of the concept of conditional probability, we present the **Monty Hall problem**. Suppose you are on a game show, and the host presents three doors before you. One of the doors has a prize behind it, and the other two doors have no prize. The host knows exactly what is behind each of the three doors, and the prize is equally likely to be hidden behind each of the doors. You are first asked to select the door that hides the prize. Then, among the two doors that you did not select, the host reveals one of them to have no prize behind it. Now, you can have what lies behind the door you originally selected, or you can switch and take what is behind the other unopened door. Using conditional probability, which door has the better chance of containing the prize?

Hint 1: Although the problem may appear symmetric at first, one of the two unopened doors will always have a higher probability of containing the prize.

Hint 2: You should switch to the other unopened door. Why? Try to consider all different possibilities.

4. Benford's Law and Voter Fraud

Suppose I make a list of the lengths of all rivers in the world, in feet. The list may include: 12, 502, 120, 206, and so on. Now, suppose I look at all of the first digits of these numbers. So I have 1, 5, 1, 2, and so on. How often will I observe each digit among $1, 2, 3, \ldots, 9$? Intuition may suggest that, since there are 9 possible digit numbers, a given river length will have a given digit roughly one ninth of the time. However, this intuition is incorrect. The river length will begin with the digit 1 about 30% of the time, 2 about 17% of the time, and 9 only about 4.5% of the time. Moreover, a similar effect occurs even if we change units to meters, or inches. And a similar effect occurs if we use base 2 numbers or base 3 numbers instead of base 10 numbers (though the exact percentages will change).

How can this be true? The intuition that we described above is incorrect. This intuition probably arose since we expected some number $n \in \mathbb{N}$ of the rivers to have length between 10 and 20, and we expect about n rivers to have length between 20 and 30, and we expect about n rivers to have length between 30 and 40, etc. However, the more accurate statement is: there are about n rivers with length between 4 and 8, there are about n rivers with length between 8 and 16, there are about n rivers with length between 16 and 32, and so on. So, the randomness occurs at an "exponential scale" rather than a "linear scale." By changing our intuition in this way, one can show (using techniques beyond this course), that in the above example, the first digit k with $1 \leq k \leq 9, k \in \mathbb{N}$ occurs with probability

$$\log_{10}\left(\frac{k+1}{k}\right)$$

This effect is known as Benford's Law.

Though it may seem a strange observation, Benford's law actually has some applications. For example, if we consider the number of votes that each candidate gets in some election in each separate voting district, then the first digits of these numbers should roughly resemble those predicted by Benford's law. So, (taking the contrapositive) if the first digits of the numbers are drastically different from Benford's law, then there is evidence of fraud in the election.

5. Cardinality of Sets

We are going to prove the following classic theorem, dating from the work of Cantor in the late 1800s.

Theorem 5.1. *There are more real numbers than rational numbers.*

We will begin by explaining the meaning of this statement. Let $n, m \in \mathbb{N}$ and consider two sets $A = \{1, \ldots, n\}$ and $B = \{1, \ldots, m\}$. How can we compare the number of elements of A and B? If $n > m$ then certainly A has more elements than B, but how do we really know this? We can try to match up the elements of A and B in a one to one correspondence. When we fail, we will see that A has more elements. Specifically, we associate $1 \in A$ to $1 \in B$, we associate $2 \in A$ to $2 \in B$, and so on, until we finally associate $m \in A$ to $m \in B$. At this point, each element of B has been associated to a distinct element of A. If we try to continue the process, we see that we have run out of elements of B to match to elements of A. However, there are still elements of A left over, since $n > m$. We conclude that A has a larger number of elements than B.

We now proceed more rigorously. Let A and B be sets in some universe. We define the notion of a function. A function f from A to B is a set of ordered pairs (a, b) such that $b \in B, a \in A$, and such that every element of A appears exactly once in this set of ordered pairs. We write $f \colon A \to B$. If (a, b) is an ordered pair for the function f, we write $f(a) = b$. We say that f is **injective** if: $\forall\ a \in A$, $\exists$ a unique $b \in B$ such that $f(a) = b$. So, negating the definition of injectivity, if f is injective, it cannot happen that $\exists\ a_1, a_2 \in A$, $a_1 \neq a_2$ such that $f(a_1) = f(a_2)$. We say that f is **surjective** if: $\forall\ b \in B$, $\exists\ a \in A$ such that $f(a) = b$.

We say that f is a **one to one correspondence** if f is injective and surjective. We say that the sets A and B have the same **cardinality** if there exists a one to one correspondence from A to B. We say that the set A has greater cardinality than B if there exists an injective function $f \colon B \to A$, but there does not exist a one to one correspondence from B to A.

For $n, m \in \mathbb{N}$ with $n > m$, $A = \{1, \ldots, n\}$ and $B = \{1, \ldots, m\}$, we showed $\exists\ f \colon B \to A$ such that f is injective. By slightly modifying the argument above, we can see that there does not exist $f \colon B \to A$ that is surjective. So, the cardinality of A is greater than the cardinality of B. Moreover, the injectivity and surjectivity properties of maps $f \colon B \to A$ tell us something about the relative sizes of the sets A and B.

Consider the identity map $f \colon \mathbb{Q} \to \mathbb{R}$ defined so that, for $q \in \mathbb{Q}$, $f(q) = q$. (Note that $\mathbb{Q}$ is contained in $\mathbb{R}$.) Let us check that f is injective. Let $q_1, q_2 \in \mathbb{Q}$ with $q_1 \neq q_2$. Then $f(q_1) = q_1 \neq q_2 = f(q_2)$. So, f is injective. Therefore, the cardinality of $\mathbb{R}$ is greater than or equal to the cardinality of $\mathbb{Q}$. To prove Theorem 5.1, we will now show that the cardinality of $\mathbb{R}$ is strictly greater than the cardinality of $\mathbb{Q}$. As a preliminary result, we show that the cardinality of $\mathbb{N}$ is equal to the cardinality of $\mathbb{Q}$.

Theorem 5.2. *The cardinality of $\mathbb{Q}$ is equal to the cardinality of $\mathbb{N}$.*

Proof. We construct an explicit one to one correspondence $f \colon \mathbb{N} \to \mathbb{Q}$. Arrange (a redundant list of) the elements of $\mathbb{Q}$ in the following doubly infinite array.

$$\begin{array}{ccccc}
1 & 1/2 & 1/3 & 1/4 & \cdots \\
2 & 2/2 & 2/3 & 2/4 & \cdots \\
3 & 3/2 & 3/3 & 3/4 & \cdots \\
4 & 4/2 & 4/3 & 4/4 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

The first row of this array $(1, 1/2, 1/3, 1/4, \ldots)$ is given the label 1, the second row of this array $(2, 2/2, 2/3, 2/4, \ldots)$ is given the label 2, and so on. The first column is this array $(1, 2, 3, 4, \ldots)$ is given the label 1, the second column of this array $(1/2, 2/2, 3/2, 4/2, \ldots)$ is given the label 2 and so on. An entry a_{ij} of the array is labelled by its row (index $i \in \mathbb{N}$)

and its column (index $j \in \mathbb{N}$). Let $k \in \mathbb{N}$. The k^{th} diagonal of the array is a set of the form $\{a_{ij} \colon i + j = k\}$. For example, the first diagonal is just the top left corner, $a_{11} = 1$. The second diagonal consists of a_{12}, a_{21}, i.e $1/2, 2$.

We now describe how to "traverse" this array. We begin with entry $1 = a_{11}$. We then move down to the number 2, and then up the second diagonal to 1/2. We then move right from 1/2 to 1/3, and then down the third diagonal (moving one entry at a time) to 3. We then move from 3 down to 4, and then up the fourth diagonal. The general procedure is: we traverse a diagonal, and then move to an adjacent endpoint of the next highest diagonal, and so on. Define $g \colon \mathbb{N} \to \mathbb{Q}$ so that $g(1) = 1$, $g(2) = 2$, $g(3) = 1/2$, $g(4) = 1/3$, $g(5) = 3$, and so on. For $n \in \mathbb{N}$, $g(n)$ is defined as the n^{th} position of our traversal of this array. (If we encounter a number that has already appeared in the array, we skip this number and move on.) By the construction of this array, every positive rational number appears in this array. Now, define $f \colon \mathbb{N} \to \mathbb{Q}$ so that $f(1) = 0$, and for $n \in \mathbb{N}$, $n > 1$, $f(2n - 2) = g(n - 1)$, $f(2n - 1) = -g(n - 1)$.

Since every positive rational number appears in the infinite array, f is surjective. Since g was selected to map onto distinct rational numbers, f is injective. Therefore, f is our desired one to one correspondence.

□

We showed above that the cardinality of $\mathbb{R}$ is greater than or equal to the cardinality of $\mathbb{Q}$. The following theorem shows that the cardinalities of $\mathbb{Q}$ and $\mathbb{R}$ are not equal. Therefore, the cardinality of $\mathbb{R}$ is strictly greater than the cardinality of $\mathbb{Q}$. That is, Theorem 5.1 follows from Theorem 5.3.

Theorem 5.3. *There does not exist a one to one correspondence between $\mathbb{Q}$ and $\mathbb{R}$.*

Proof. Before we begin, let us fix a definition of the real numbers $\mathbb{R}$. It suffices to define $\mathbb{R}$ as the set of infinite decimals of the form $r = s \cdot b_n b_{n-1} \cdots b_0.a_1 a_2 a_3 a_4 \cdots$, where $n \in \mathbb{Z}$, $n \geq 0$, $s \in \{-1, 1\}$, for all $i \in \mathbb{Z}$, $a_i \in \mathbb{Z}$, $0 \leq a_i \leq 9$, for all $i \in \{1, 2, \ldots, n\}$, $b_i \in \mathbb{Z}$, $1 \leq b_i \leq 9$, $b_0 \in \mathbb{Z}$, $0 \leq b_0 \leq 9$, and such that the following does not occur: there exists $N \in \mathbb{N}, N > 0$ such that, for all $j > N$, $a_j = 9$. That is, we do not allow a constant, infinite sequence of 9's. Since we want the real numbers to be uniquely represented as infinite decimals, the fact that $0.9999999\ldots$ and 1 represent the same number is not desirable, so we eliminate one of these two representatives.

We now argue by contradiction. Suppose there exists a one to one correspondence $g \colon \mathbb{Q} \to \mathbb{R}$. From Theorem 5.2, there exists a one to one correspondence $h \colon \mathbb{N} \to \mathbb{Q}$. Define $f \colon \mathbb{N} \to \mathbb{R}$ so that $f(n) = g(h(n))$. Then f is a one to one correspondence. Suppose we enumerate the elements of f. For example, we have

$$\begin{aligned}
&f(1) = 2348.234203549\ldots\\
&f(2) = -123.849300000002343200\ldots\\
&f(3) = 1\\
&f(4) = 3.14159265358979323846264\ldots\\
&f(5) = -1.000234938989328\ldots\\
&\quad\ldots
\end{aligned}$$

Let us fix labels to the digits, so that

$$\begin{aligned}
f(1) &= b_{3,1}b_{2,1}b_{1,1}b_{0,1}.a_{1,1}a_{2,1}a_{3,1}a_{4,1}a_{5,1}a_{6,1}\ldots\\
f(2) &= -b_{2,2}b_{1,2}b_{0,2}.a_{1,2}a_{2,2}a_{3,2}a_{4,2}a_{5,2}a_{6,2}\ldots\\
f(3) &= b_{0,3}.a_{1,3}a_{2,3}a_{3,3}a_{4,3}a_{5,3}a_{6,3}\ldots\\
f(4) &= b_{0,4}.a_{1,4}a_{2,4}a_{3,4}a_{4,4}a_{5,4}a_{6,4}\ldots\\
f(5) &= -b_{0,5}.a_{1,5}a_{2,5}a_{3,5}a_{4,5}a_{5,5}a_{6,5}\ldots\\
&\ldots
\end{aligned}$$

In particular, for $i,j\in\mathbb{Z}$, $i,j\geq 0$, $0\leq b_{i,j},a_{i,j}\leq 9$, $b_{i,j},a_{i,j}\in\mathbb{Z}$. We now construct a real number y such that, for all $n\in\mathbb{N}$, $f(n)\neq y$. The existence of such a y violates the surjectivity of f.

Let $y=b.a_1a_2a_3a_4\cdots$, so that $b=1$, $a_1\neq a_{1,1}$, $a_2\neq a_{2,2}$, $a_3\neq a_{3,3}$, $a_4\neq a_{4,4}$, and so on. In general, for $n\in\mathbb{N}$, choose $a_n\neq a_{n,n}$ and such that $1\leq a_n\leq 8$. Then y is a real number, and by the definition of y, y cannot be equal to any number $f(n)$, $n\in\mathbb{N}$. The surjectivity of f is therefore violated. Since we have achieved a contradiction, we conclude that no such g exists. That is, there is no one to one correspondence $g\colon\mathbb{Q}\to\mathbb{R}$. □

Courant Institute, New York University, New York NY 10012
E-mail address: heilman@cims.nyu.edu