

Lecture 4: The Technique of Proof

1 The Technique of Proof

In our first lecture, we discussed what it means to prove a statement in mathematics. Specifically, we talked not just about what it means for a mathematical statement to be a proof, but what it means for a mathematical statement to be a **good** proof; i.e. mathematically we wanted our proofs to not just be logically consistent and made of true statements, but we also wanted our proofs to be illuminating and to teach us something about the statements we're studying. Since then, we've studied the practice of how these proofs get implemented by examining the real and rational number systems, coming up with specialized tools (bijections) and techniques (diagonalization) to prove claims in these systems.

For the last lecture of our class, instead of introducing a mathematical object and coming up with proof methods to attack it, we're going to attempt the converse; we're going to introduce promising mathematical techniques, and then discuss their uses and applications. We start with the concept of "proof by contradiction:"

1.1 Proofs by Contradiction

The best way to illustrate the idea behind a proof by contradiction is to consider an example.

Theorem. There are two irrational numbers a and b such that a^b is rational.

Proof. So: if we wanted to directly prove that such a pair of numbers existed, we would need to actually concretely exhibit a pair of irrational numbers a, b such that a^b was rational. The difficulty with this approach, frustratingly, is that we don't really know of many irrational numbers at this point in time! In our class yesterday, we proved that the $\sqrt[3]{2}$ was irrational, and in the HW you also proved that $\sqrt{2}$ is irrational; however, we really don't have many other examples! As well, we don't really have any techniques for actually calculating what a^b is, for non-rational values of a, b ; therefore, this direct approach seems difficult.

Instead, consider the following way to "side-step" these difficulties: instead of attempting to explicitly find such a pair of numbers a, b , we can instead prove that it is impossible for our claim to fail: i.e. that it cannot be that for every pair of irrational numbers a, b , a^b is also irrational. At first, this seems like a colossal misstep; we've turned a search for one pair of irrational numbers into a claim made about **every** pair of irrational numbers. However, suppose we look at our situation this way:

- We have a claim we're trying to prove; let's denote it P , for shorthand.
- Instead of proving P is true directly, we want to prove that $\neg P$ is impossible (i.e. false.)

- To do this, we can simply do the following:
 1. Assume, for the moment, that $\neg P$ is actually true!
 2. Working from this assumption, find a pair of contradictory statements that are implied by $\neg P$; i.e. a pair of statements $Q, \neg Q$ such that $P \Rightarrow Q$ and $P \Rightarrow \neg Q$. Common examples are $Q = "1 = 0"$, or $Q(n) = "n \text{ is even}"$ or other such things.
 3. This proof demonstrates that $\neg P$ must be impossible, because it implies two contradictory things (like the two simultaneous claims $Q(n) = "n \text{ is even}"$ and $\neg Q(n) = "n \text{ is odd.}"$) Mathematics is free from contradictions by design¹; therefore, we know that this must be impossible, i.e. that $\neg P$ must be false, i.e. that P must be true!

In general, this is how a **proof by contradiction** works;² take your claim P , assume it's false, and use $\neg P$ to deduce a pair of contradictory statements, which you know mathematics cannot contain.

In the example we're studying here, we want to show that it's impossible for a^b to be irrational for every pair of irrational numbers a, b . To do this via a proof by contradiction, we do the following: first, assume that a^b is irrational for every pair of irrational numbers a, b . If we apply this knowledge to one of the few numbers ($\sqrt{2}$) we know is irrational, our assumption tells us that in specific

$$\sqrt{2}^{\sqrt{2}} \text{ is irrational.}$$

What do we do from here? Well: pretty much the only thing we have is our assumption, our knowledge that $\sqrt{2}$ is irrational, and our new belief that $\sqrt{2}^{\sqrt{2}}$ is **also** irrational. The only thing really left to do, then, is to let $a = \sqrt{2}^{\sqrt{2}}$, $b = \sqrt{2}$, and apply our hypothesis again. But this is excellent! On one hand, our we have that a^b is irrational by our hypothesis. On the other hand, we have that a^b is equal to

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2,$$

which is clearly rational. This is a contradiction! Therefore, we know that our hypothesis must be false: there must be a pair of irrational numbers a, b such that a^b is rational. \square

An interesting quirk of the above proof is that it didn't actually give us a pair of irrational numbers a, b such that a^b is rational! It simply told us that either

- $\sqrt{2}^{\sqrt{2}}$ is rational, in which case $a = b = \sqrt{2}$ is an example, or
- $\sqrt{2}^{\sqrt{2}}$ irrational, in which case $a = \sqrt{2}^{\sqrt{2}}, b = \sqrt{2}$ is an example,

¹This is why we tried to insure that we only start with true statements in our proofs.

²A beautiful quote about proofs by contradiction, by the mathematician G. H. Hardy: “[Proof by contradiction], which Euclid loved so much, is one of a mathematician’s finest weapons. It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game.”

but it never actually tells us which pair satisfies our claim! This is a weird property of proofs by contradiction: they are often **nonconstructive** proofs, in that they will tell you that a statement is true or false without necessarily giving you an example that demonstrates the truth of that statement.

1.2 Proofs by Contrapositive

The structure of a proof by contrapositive is remarkably simple: suppose we want to prove some statement of the form $P \Rightarrow Q$. Sometimes, this kind of a statement can be rather tricky to prove: perhaps P is a really tricky condition to start from, and we would prefer to start working from the other end of this implication. How can we do this?

Via the **contrapositive**! Specifically, if we have a statement of the form $P \Rightarrow Q$, the contrapositive of this statement is simply the statement

$$\neg Q \Rightarrow \neg P.$$

The nice thing about the contrapositive of any statement is that it's **exactly the same** as the original statement! For example, if our statement was “all Mathcampers are not soluble in water,” the contrapositive of our claim would be the statement “anything that is soluble in water is not a Mathcamper.” These two statements clearly express the same meaning – one just starts out by talking about Mathcampers, while the other starts out by talking about things that you can dissolve in water. So, if we want to prove a statement $P \Rightarrow Q$, we can always just prove the contrapositive $\neg Q \Rightarrow \neg P$ instead, because they're the same thing! This can allow us to switch from relatively difficult starting points (situations where P is hard to work with) to easier ones (situations where $\neg Q$ is easy to work with.) In particular, in the example above, working with the statement “all Mathcampers are soluble in water” will make a brute-force proof much easier: it is far easier to drop every Mathcamper in a lake than to check every soluble object to see if it's been to Mathcamp recently.

To illustrate this, consider the following example:

Theorem. Let n be a natural number. Then, if $n \equiv 2 \pmod{3}$, n is not a square: in other words, we cannot find any integer k such that $k^2 = n$. (We write that $a \equiv b \pmod{c}$ if $a - b$ is a multiple of c : in other words, that a and b are the “same” up to some number of copies of c .)

Proof. A direct approach to this problem looks . . . hard. Basically, if we were to prove this problem directly, we would take any $n \equiv 2 \pmod{3}$ – i.e. any n of the form $3m + 2$, for some integer m – and try to show that this can never be a square. Basically, we'd be looking at the equation $k^2 = 3m + 2$ and trying to show that there are no solutions to this equation, which just looks kind of . . . ugly, right?

So: because we are mathematicians, we are **lazy**. In particular, when presented with a tricky-looking problem, our instincts should be to try to make it trivial: in other words, to attempt different proof methods and ideas until one seems to “fit” our question. In this case, as suggested by our section title, let's attempt to prove our theorem by studying its contrapositive:

$$\text{If } n \text{ is a square, then } n \not\equiv 2 \pmod{3}.$$

Equivalently, because every number is equivalent to either 0, 1, or 2 mod 3, we're trying to prove the following:

If n is a square, then $n \equiv 0$ or $1 \pmod{3}$.

This is now a much easier claim! – the initial condition is really easy to work with, and the later condition is rather easy to check.

Now that we have some confidence in our ability to prove our theorem, we proceed with the actual work: take any square n , and express it as k^2 , for some natural number k . We can break k into three cases:

1. $k \equiv 0 \pmod{3}$. In this case, we have that $k \equiv 3m$ for some m , which means that $k^2 = 9m^2 = 3(3m^2)$ is also a multiple of 3. Thus, $k^2 \equiv 0 \pmod{3}$.
2. $k \equiv 1 \pmod{3}$. In this case, we have that $k \equiv 3m + 1$ for some m , which means that $k^2 = 9m^2 + 6m + 1 = 3(3m^2 + 2m) + 1$. Thus, $k^2 \equiv 1 \pmod{3}$.
3. $k \equiv 2 \pmod{3}$. In this case, we have that $k \equiv 3m + 2$ for some m , which means that $k^2 = 9m^2 + 12m + 4 = 3(3m^2 + 4m + 1) + 1$. Thus, $k^2 \equiv 1 \pmod{3}$.

Therefore, we've shown that k^2 isn't congruent to 2 mod 3, for any k . So we've proven our claim! □

1.3 Proofs of Equivalence

Another common proof technique comes up when we're trying to prove two statements are equivalent. For example, suppose that we have the following two statements:

- $P(x, y) = "(x + 1)^2 = (y + 1)^2."$
- $Q(x, y) = "x + y = -2,"$ or $x = y."$

As it turns out, these two statements are equivalent: i.e. $P(x, y) \Leftrightarrow Q(x, y)$. How can we prove this? Well, one useful blueprint for such a proof is the following:

- First, show that $P(x, y) \Rightarrow Q(x, y)$: i.e. that if we assume $P(x, y)$ is true, then we can conclude that $Q(x, y)$ is also true.
- Then, show the opposite direction: that $Q(x, y) \Rightarrow P(x, y)$! I.e. we will assume that $P(x, y)$ is true, and attempt to prove that $Q(x, y)$ is also true.

If we have done this, we will have proven that $P(x, y)$ is true if and only if $Q(x, y)$ is also true: i.e. that $P(x, y) \Leftrightarrow Q(x, y)$! Excellent. Now, let's actually do this for these two statements, to illustrate how such a proof works:

$P(x, y) \Rightarrow Q(x, y)$: Assume that $P(x, y)$ holds: i.e. that $(x + 1)^2 = (y + 1)^2$. Then, by taking square roots of both sides, we have that

$$(x + 1) = \pm(y + 1),$$

where the \pm is because there are two possible square roots for any positive number, either its positive square root or that same positive square root times (-1) . So: if

$$(x + 1) = +(y + 1),$$

then subtracting 1 from both sides gives us $x = y$, which is one possible way to make $Q(x, y)$ true. Otherwise, if

$$(x + 1) = -(y + 1),$$

we can add y to both sides and subtract 1 from both sides to get $x + y = -2$, which is another way to make $Q(x, y)$ true. Therefore, in either case, if $P(x, y)$ is true, so is $Q(x, y)$!

$Q(x, y) \Rightarrow P(x, y)$: There are two different ways to make $Q(x, y)$ true: either set $x = y$ or set $x + y = -2$, i.e. $x + 1 = -(y + 1)$. In either case, we have that $(x + 1)^2 = (y + 1)^2$, so we know that $P(x, y)$ is true.

Therefore, we've shown that $P(x, y) \Leftrightarrow Q(x, y)$.

1.4 Proofs by Induction

Sometimes, in mathematics, we will want to prove the truth of some statement $P(n)$ that depends on some variable n . For example:

- $P(n) =$ "The sum of the first n natural numbers is $\frac{n(n+1)}{2}$."
- $P(n) =$ "If $q \geq 2$, we have $n \leq q^n$."
- $P(n) =$ "Every polynomial of degree n has at most n roots."

For any fixed n , we can usually use our previously-established methods to prove the truth or falsity of the statement. However, sometimes we will want to prove that one of these statements holds for **every** value $n \in \mathbb{N}$. How can we do this?


One method for proving such claims for every $n \in \mathbb{N}$ is the method of **mathematical induction!** Proofs by induction are somewhat more complicated than the previous two methods. We sketch their structure below:

- To start, we take our claim $P(n)$, that we want to prove holds for every $n \in \mathbb{N}$.
- The first step in our proof is the **base step**: in this step, we explicitly prove that the statement $P(1)$ holds, using normal proof methods.
- With this done, we move to the **induction step** of our proof: here, we prove the statement $P(n) \implies P(n + 1)$, for every $n \in \mathbb{N}$. This is an implication; we will usually prove it directly by assuming that $P(n)$ holds and using this to conclude that $P(n + 1)$ holds.

Once we've done these two steps, the principle of induction says that we've actually proven our claim for all $n \in \mathbb{N}$! The rigorous reason for this is the **well-ordering principle**, which we discussed in class; however, there are perhaps more intuitive ways to think about induction as well.

The way I usually think of inductive proofs is to think of **toppling dominoes**. Specifically, think of each of your $P(n)$ propositions as individual dominoes – one labeled $P(1)$, one labeled $P(2)$, one labeled $P(3)$, and so on/so forth. With our inductive step, we are insuring that all of our dominoes are *lined up* – in other words, that if one of them is true, that it will “knock over” whichever one comes after it and force it to be true as well! Then, we can think of the base step as “knocking over” the first domino; once we do that, the inductive step makes it so that all of the later dominoes also have to fall, and therefore that our proposition must be true for all n (because all the dominoes fell!)

To illustrate how these kinds of proofs go, here’s an example:

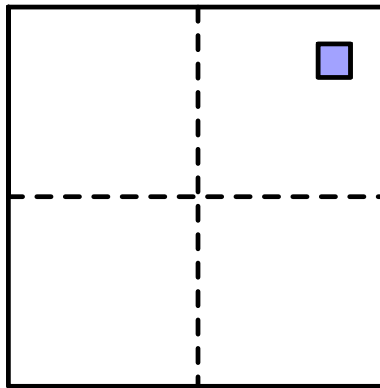
Claim 1. For any $n \in \mathbb{N}$, take a $2^n \times 2^n$ grid of unit squares, and remove one square from somewhere in your grid. The resulting grid can be tiled by  - shapes.

Proof. As suggested by the section title, we proceed by induction.

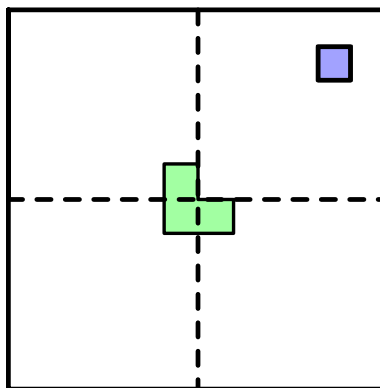
Base case: for $n = 1$, we simply have a 2×2 grid with one square punched out. As this *is* one of our three-square shapes, we are trivially done here.

Inductive step: Assume that we can do this for a $2^k \times 2^k$ -grid without a square, for any $k \leq n$. We then want to prove that we can do this for a $2^{n+1} \times 2^{n+1}$ grid minus a square.

So: take any such grid, and divide it along the dashed indicated lines into four $2^n \times 2^n$ grids. By rotating our grid, make it so that the one missing square is in the upper-right hand corner, as shown below:



Take this grid, and carefully place down one three-square shape as depicted in the picture below:



Now, look at each of the four $2^n \times 2^n$ squares in the above picture. They all are missing exactly one square: the upper-right hand one because of our original setup, and the other three because of our placed three-square-shape. Thus, by our inductive hypothesis, we know that all of these squares can also be tiled! Doing so then gives us a tiling of the whole shape; so we've created a tiling of the $2^{n+1} \times 2^{n+1}$ grid!

As this completes our inductive step, we are thus done with our proof by induction. \square

The above question – one where you are in some sense “growing” or “extending” a result on smaller values of n to get to larger values of n – is precisely the kind of question that induction is set up to solve. The following problem about the Fibonacci numbers is another such “extending” problem:

Definition. The n -th **Fibonacci number** is defined recursively as follows:

- $f_0 = 0$.
- $f_1 = 1$.
- $f_n = f_{n-2} + f_{n-1}$.

Examples. Here is the start of the Fibonacci number sequence:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \dots$$

Claim 2. *The n -th Fibonacci number is even iff n is a multiple of 3.*

Proof. As noted above, the “recursive” construction of the Fibonacci numbers, where it looks like we’re building our numbers out of earlier-defined numbers, suggests induction.

So: let’s try! Our base case for a number of immediate cases is trivially true: we can check by hand that $f_0 = 0$, $f_1 = 1$, and $f_2 = 1$.

So: inductively, suppose we know that f_n is even if and only if n is a multiple of 3. Does this help us with f_{n+1} ?

The answer is ... no, not really. Because

$$f_{n+1} = f_n + f_{n-1},$$

we really need more information than just f_n : we also need to know whether f_{n-1} is even or odd! Our normal induction isn’t strong enough here; we need something...stronger. Like ... **strong** induction!

Strong induction proceeds very similarly to normal induction:

- To start, we take our claim $P(n)$, that we want to prove holds for every $n \in \mathbb{N}$.
- The first step in our proof is the **base step**: in this step, we explicitly prove that the statement $P(1)$ holds, using normal proof methods.
- With this done, we move to the **induction step** of our proof. For strong induction, we prove the statement that the combined statements $P(1) \wedge P(2) \wedge \dots \wedge P(n)$ implies $P(n+1)$. If you go back to our domino analogy, this is like asking whether knowing that **every** domino from 1 to n falling over tells you that the $n+1$ -th domino falls over.

So: if we're using strong induction, then we're allowed to assume that our inductive hypothesis holds for every value between 0 and n , and prove that it holds for $n + 1$. We know that

$$f_{n+1} = f_n + f_{n-1};$$

so, it suffices to consider the three possible cases for $n + 1$. Either $n + 1$ is a multiple of 3, in which case we can write it as $3k$, or it is 1 mod 3, in which case it can be written as $3k + 1$, or it's 2 mod 3, in which case we can write it as $3k + 2$. In any case, we can use our inductive hypothesis to see that

$$\begin{aligned} f_{3k} &= f_{3k-1} + f_{3k-2} = \text{odd} + \text{odd} = \text{even}, \\ f_{3k+1} &= f_{3k} + f_{3k-1} = \text{even} + \text{odd} = \text{odd}, \\ f_{3k+2} &= f_{3k+1} + f_{3k} = \text{odd} + \text{even} = \text{odd}, \end{aligned}$$

and thus that our property holds in any of these three cases. Thus, by induction, we know that f_n is even if and only if it is a multiple of 3. \square

1.5 Combinatorial Proofs

A **combinatorial proof**, roughly speaking, is a way of proving an equality of the form $A = B$ by finding some collection which when counted in one fashion yields A and when counted in a different fashion yields B . Because the number of elements in the collection is the same regardless of how they're counted, this tells us that $A = B$. This sounds more abstract than it really is; so, to illustrate, let's calculate a few examples:

Definition. Suppose we have a collection of n distinct objects and we choose k distinct things from this collection, not paying attention to the order we choose them in. In how many different ways can we do this?

Well: let's pick elements one by one. We have n choices for the first thing we pick, $n - 1$ choices for the second thing we pick (because we already removed the first object), $n - 2$ for the third, and so on/so forth until we have $n - k + 1$ many choices for the k -th thing we pick.

However, we want to not pay attention to the order we chose these things in. There are $k \cdot (k - 1) \cdot \dots \cdot 1$, which we denote as $k!$ for shorthand, many different ways to order any collection of k distinct elements. Therefore, each possible set we can pick shows up $k!$ -many times in the ordered count we perform above. Therefore, if we want to disregard the order, we can simply divide through by $k!$. In other words, there are

$$\frac{n \cdot (n - 1) \cdot \dots \cdot (n - k + 1)}{k!} = \frac{n!}{(n - k)! \cdot k!}$$

many ways to choose k elements from a collection of n distinct objects without caring about order. This quantity comes up in tons of different fields of mathematics; we denote it as $\binom{n}{k}$, and call such numbers **binomial coefficients**.

Claim 3. For any $n, k \in \mathbb{N}$, $k < n$, we have $\binom{n}{k} = \binom{n}{n-k}$.

Proof. We simply count in two ways the number of ways to choose a set of size k from a set of size n without caring about order. On one hand, we know that this is just $\binom{n}{k}$, from our discussion above. However, choosing the elements to take for subset of size k is precisely the same as choosing the elements to **not take** for that same subset: i.e. it's the same as choosing $n - k$ elements to **not pick**. But there are precisely $\binom{n}{n-k}$ many ways to pick this set of “unchosen” elements. Because both arguments are counting the same thing, we have that $\binom{n}{k} = \binom{n}{n-k}$, as claimed. \square

Claim 4.

$$\sum_{k=0}^n \binom{n}{k} = 2^n.$$

Proof. To see this, consider the following third and seemingly unrelated question: given a set of n people, in how many ways can we form a committee out of them? (Allowing the empty committee consisting of 0 people as a valid option.)

On one hand, we can see that there are 2^n many possible committees: each person has 2 choices, the option to either be in a committee or not, there are n people, and each set of different choices corresponds to a different committee.

On the other hand, suppose we think about this in terms of the overall sizes of the committees. Specifically: for any k , the number of committees that can be formed with k members is precisely $\binom{n}{k}$, the number of ways to pick k people out of our set of n people. Therefore, the total number of committees is just the sum of these binomial coefficients over all of the possible committee sizes: i.e. $\sum_{k=0}^n \binom{n}{k}$. Therefore, we have

$$\sum_{k=0}^n \binom{n}{k} = 2^n,$$

as claimed. \square

1.6 Pigeonhole Proofs

Finally, we close with the pigeonhole principle, a rather unassuming property that has some remarkable applications:

Proposition. (Pigeonhole principle, simple version): Suppose that $kn + 1$ pigeons are placed into n pigeonholes. Then some hole has at least $k + 1$ pigeons in it.

Proof. The most pigeons that can be put into n holes so that no hole has more than k pigeons is kn . Adding more than that many pigeons must necessarily result in a hole with $k + 1$ pigeons. \square

The applications of this property are where it really shines. We calculate one silly example and one more serious one:

Claim 5. Suppose that “friendship” is³ a symmetric relation: i.e. that whenever a person A is friends with a person B , B is also friends with A . Also, suppose that you are never friends with yourself (i.e. that friendship is antireflexive.) Then, in any set S of greater than two people, there are at least two people with the same number of friends in S .

Proof. Let $|S| = n$. Then every person in S has between 0 and $n - 1$ friends in S . Also notice that we can never simultaneously have one person with 0 friends and one person with $n - 1$ friends at the same time, because if someone has $n - 1$ friends in S , they must be friends with everyone besides themselves.

Therefore, each person has at most $n - 1$ possible numbers of friends, and there are n people total: by the pigeonhole principle, there must be some pair of people whose friendship numbers are equal. \square

Definition. A **sequence** of real numbers is a subset of the real numbers together with some order in which they’re written down. Typically, we will write a sequence of length n as (r_1, r_2, \dots, r_n) , where r_i denotes the i -th element.

A **subsequence** of a sequence is a way to pick out some of the elements from this set while still keeping them in the order given by the collection. For example, one possible subsequence of the sequence $\{9, 2, 5, 0, 1, 6\}$ could be $\{2, 0, 1\}$.

A subsequence is called **monotone** if its terms form either an increasing or decreasing list when taken in order: i.e. while the subsequence $\{2, 0, 1\}$ we looked at earlier is not monotone, the subsequences $\{9, 5, 0\}$ and $\{0, 1, 6\}$ are monotone.

Claim 6. Take any sequence S of $n^2 + 1$ distinct real numbers $(r_1, r_2, \dots, r_{n^2+1})$. Then there is a monotone sequence of S of length $n + 1$.

Proof. For each k between 1 and $n^2 + 1$, let x_k be the length of the longest increasing subsequence starting with r_k , and y_k be the length of the longest decreasing subsequence starting with r_k . If there is no monotone subsequence of length $n + 1$, then these values range from 1 to n : therefore, if we look at the pairs (x_k, y_k) , there are at most n^2 many possible distinct pairs. Therefore, by the pigeonhole principle, there must be some pair of values j, k such that $(x_k, y_k) = (x_j, y_j)$.

However, is this actually possible? Look at the values r_k, r_j . There are two possibilities: $r_k < r_j$ or $r_k > r_j$. If $r_k < r_j$, then we can actually make an increasing subsequence of length $x_j + 1$ by starting at r_k and then taking the subsequence of length x_j that starts at r_j . But this contradicts our claim that x_k was the length of the longest increasing subsequence starting at k ! Similarly, if $r_k > r_j$, we can make a decreasing subsequence of length $y_j + 1$ by starting with r_k and then taking the subsequence of length y_j starting at r_j . This is again a contradiction: therefore, we know that this original setup (that such a pair $(x_k, y_k) = (x_j, y_j)$ exists) must be impossible.

Therefore, because we cannot have such a pair, the pigeonhole principle tells us that there must be a monotone subsequence of length at least $n + 1$, as claimed. \square

³Magic!