Discrete Math Lecture 2

1 Methods of proof

> I know that 2 and 2 make 4 - and should be glad to prove it too if I could - though I must say if by any sort of process I could convert 2 and 2 into 5 it would give me much greater pleasure.
>
> - Lord Byron

Proving things in mathematics can be a very creative process. In the search for proofs, there is not a guaranteed path to success. For example, in the summer of 1742, a German mathematician by the name of Christian Goldbach wondered whether every even integer greater than 2 could be written as the sum of two primes. Centuries later, we still don't have a proof of this (computers have checked that Goldbach's Conjecture holds for all numbers less than 4×10^{18} which leaves only infinitely many more numbers to check).

Writing proofs is a bit of an art. Like any art, to be truly great at it, you need some sort of inspiration, but also some foundational technique. Just as painters can learn the proper way to hold a brush, we can look at proper ways to construct arguments. Today we will look at a bunch of proofs and see various ways in which we can prove things.

Most theorems look something like

If statement p is true, then statement q is true.

Thankfully with our knowledge about implications we can already suggest two methods of proof:

- (Direct proof) Start with p. Apply a chain of logical steps to get to q.
- (Proof by contrapositive) We know that an implication is equivalent to its contrapositive. The contrapositive of

  If statement p is true, then statement q is true.

  is

  If statement $\neg q$ is true, then $\neg p$ is true.

  So we can start with $\neg q$ and apply a chain of logical steps to get to $\neg p$. This proves the desired result that if statement p is true, then statement q is true.

  Note that p and q can and often will be complex expressions that may also be quantified, so we will need to use both DeMorgan's laws as well as our rules about negating quantified expressions in order to effectively use the method of taking the contrapositive.

1.1 Direct proof

This is the most straight-forward of the proof methods. We begin with the premise or assumptions of the theorem and step by step reason our way to the conclusion. Let's say that here we are considering variables that can take values from some set S. To show that $\forall x, p(x) \implies q(x)$ we need to argue that for each and every $x \in S$, $p(x) \implies q(x)$. Often this is done by considering an arbitrary x and showing $p(x) \implies q(x)$. Since we don't use anything special that would distinguish this x from any other element in S, this is legitimate. Our reasoning would work for each and every $x \in S$.

Proposition 1. *For any natural number n, n is even $\implies$ n^2 is even.*

Proof. Consider an arbitrary natural number n that is even. It must be a multiple of 2. So $n = 2k$ for some other natural number k. But then $n^2 = 4k^2 = 2 \times (2k^2)$. Since k is a natural number, so is $2k^2$. Thus, n^2 is a multiple of 2 and hence is a natural number. □

Case by case proof Sometimes the premise p might consist of a bunch of cases in the following form: $p = p_1 \vee p_2 \vee \ldots \vee p_k$. Suppose $p = p_1 \vee p_2 \vee p_3$. Then to prove $p \implies q$, i.e.,

$$p_1 \vee p_2 \vee p_3 \implies q$$

, it is sufficient to prove that $p_1 \implies q$, $p_2 \implies q$ and $p_3 \implies q$ separately. This is because to show $p \implies q$ is true, we need to argue that whenever p holds, so does q. But if p holds and $p = p_1 \vee p_2 \vee p_3$, then one of the three cases, p_1, p_2 or p_3, must hold. No matter which one is true, we know that q is true since the cases each individually imply q.

Note that p might not be already written in terms of the OR of a bunch of case, but it might be useful to us to write it in this way and then do a proof by cases. One common example of this is that if we want to show some statement S holds, with no other premise, we can define some suitable proposition A and show that both $A \implies S$ and $\neg A \implies S$. Since $A \vee \neg A$ always holds, we can safely "assume" this and then do a proof by cases, showing that both $A \implies S$ and $\neg A \implies S$. Here is an example of this.

Proposition 2. *For any natural number n, $n^2 + n$ is even.*

Proof. First note that $n^2 + n = n(n+1)$. We will now consider two cases, one where n is odd and the other when n is even. These two cases are complements of each other: n cannot be neither odd nor even. So now we just have to prove in both the cases, that $n(n+1)$ is even.

- n is even: then n is a multiple of 2, so $n = 2k$ for some other natural number k. But then $n(n+1) = 2k(n+1)$ so $n(n+1)$ is also a multiple of 2 (since $k(n+1)$ is a natural number) and so $n(n+1)$ is even.
- n is odd: then $n+1$ is even. So $n+1 = 2k$ for some other natural number k. But then $n(n+1) = 2nk$ which is a multiple of 2 and hence even.

□

Hilariously, this method is also sometimes called proof by exhaustion. It's not because you will become exhausted over the course of writing the proof; but rather because you "exhaust" all possible cases and show that the result follows in each case.

1.2 Proving the contrapositive

We already saw an example in the last class where proving $p \implies q$ seems hard but proving $\neg q \implies \neg p$ was easier. But, as we already know, these two things are equivalent. Thus we can happily prove $\neg q \implies \neg p$ in order to prove $p \implies q$. Here is another example

Proposition 3. *Prove that if the side lengths of a triangle are 1, 2 and 3, then the triangle cannot be right-angled.*

Proof. Let

$$p = \text{“the side lengths of a triangle are 1, 2 and 3”}$$

and

$$q = \text{“the triangle cannot be right-angled”}$$

If we want to directly prove $p \implies q$, one way is to calculate what the triangle's angles are and say that no angle is 90 degrees. But this might need some trigonometry. Let's say we don't remember how to calculate the angles of a triangle using the side lengths. But we do remember the simpler Pythagoras formula for the side lengths of a right angled triangle: the side lengths will satisfy $a^2 + b^2 = c^2$ where a, b and c are the side lengths.

We can now prove the contrapositive: $\neg q \implies \neg p$ instead. Assume $\neg q$. That means the triangle is right angled. Then the side lengths cannot be 1,2 and 3 because $1^2 + 2^2 \neq 3^2$. We have shown $\neg p$ and completed the task of proving the contrapositive. □

1.3 Proof by contradiction

> “When you have eliminated the impossible, whatever remains, however improbable, must be the truth.”
>
> - Sherlock Holmes, *The Sign of the Four (1890)*

Proof via contradiction is similar to a proof by counterexample, but it can be used even when it isn't clear how to phrase your theorem as an implication in a natural way. Consider a statement like

“There is no largest natural number”

How would you phrase this as an implication? It seems very awkward. So we will instead proceed by way of contradiction. This method can be used to prove a proposition p in the following manner.

- Assume $\neg p$.
- Proceed with a sequence of logical steps till you end up at a proposition that is known to be false. This is your contradiction.
- Conclude that p must be true.

Why is this correct reasoning. Well, intuitively, you have assumed $\neg p$ and then proceeded with correct rules of reasoning. This led you to a false conclusion. But the rules you followed were correct, so your premises must have been wrong. But you only used $\neg p$ and all other facts you used were valid. So $\neg p$ must have been false. Here is an example of such a proof.

Proposition 4. *There is no largest natural number.*

Proof. By way of contradiction say there was a largest natural number. Call it L. Then $L + 1$ is a natural number strictly bigger than L. This violates the fact that L is the largest natural number, which we assumed. This completes the proof by contradiction. □

This proof is also an example of using another idea: the extremal principle, which we shall see later. It also illustrates that when you prove p by contradiction, you assume $\neg p$ and try to reach something known to be false. In particular reaching p is good enough since you already assumed $\neg p$ to be true and now you have shown p is true, but we know that both p and it's complement can't both be true. $p \wedge \neg p$ is the contradiction.

Excercise 1. *In fact assuming $\neg(p \implies q)$ and deducing $\neg p$ suffices to complete a proof by contradiction that $p \implies q$. Why? Look at the proof by contradiction of the pigeonhole principle given below and convince yourself of this.*

Statements of the form $p \implies q$ can also be proven via contradiction. We can assume $\neg(p \implies q)$ and arrive at a contradiction. Generally such proofs can also be done by considering the contrapositive of $p \implies q$ and proving that instead. You can choose to use either the contrapositive method, or the proof by contradiction method depending on your preference.

The difference is subtle. To prove $p \implies q$

- By contrapositive: Prove $\neg q \implies \neg p$ instead. That is assume $\neg q$ and derive $\neg p$.
- By contradiction: Assume $\neg(p \implies q)$ and derive something that is known to be false.

Here is an example of this:

Proposition 5 (Pigeon hole principle)**.** *Let k be a natural number. Suppose you have $k+1$ pigeons that live in k pigeonholes. Then at least one pigeonhole has more than one pigeon in it.*

Let

$$p = \text{“There are } k+1 \text{ pigeons in } k \text{ pigeonholes”}$$

and

$$q = \text{“There exists a pigeonhole with multiple pigeons in it”}$$

By proving the contrapositive. We will prove $\neg q \implies \neg p$. By DeMorgans' Law:

$$\neg q = \text{All pigeon holes have at most one pigeon in them}$$

But then there can be at most k pigeons since even if every pigeonhole had one pigeon, there are only k pigeonholes. Thus there are not $k+1$ pigeons. This proves $\neg p$, completing the proof by proving the contrapositive.

□

By contradiction. Suppose the implication is false. That is assume $\neg(p \implies q)$. The only way this implication can be false is if p is true and q is false, assuming this is the same as assuming the proposition $p \wedge \neg q$ is true. That is to say by assuming that the implication we want to prove is false, we are assuming $p \wedge \neg q$ is true. That is, there are $k+1$ pigeons but each pigeonhole contains at most one pigeon. But imagine sending the pigeons to their pigeon holes one-by-one. Once a single pigeon goes to a pigeon hole we can no longer use that pigeon hole. We start with one more pigeon than pigeon hole, so we will not be able to fit every pigeon into a pigeon hole. So we have deduced $\neg p$. But we assumed $p \wedge \neg q$ However both these cannot hold at the same time, since $p \wedge \neg q \wedge \neg p = 0 \wedge \neg q = 0$. Thus we arrive at a contradiction.

□

The proofs here are not completely formal, to be more precise we can use the idea of a bijection, which will also come up later in the class. This principle sounds extraordinarily obvious but has a surprising number of powerful applications. We will see more of it later in the class. Meanwhile the etymology section of this Wikipedia article offers some explanation of the oddly specific term ‘pigeonhole’ in this context.

1.4 Proof by counterexample(?!)

You **cannot** prove a statement like $\forall x \in \mathbb{N}, P(x)$ by showing $P(x)$ is true for any finite number of examples. This is not to say that looking at examples is a waste of time. Doing so will often give you an idea of how to write a proof. But the examples do not belong in the proof.

However, it is possible to prove statements such as existential statements by means of demonstrating just a single example. In particular a statement like $\forall x \in \mathbb{N}, P(x)$ can be disproved by showing the existence of a single counterexample. For instance if we want to prove that there is an integer n such that $n^2 - n + 41$ is not prime, all we need to do is find one. This might seem like a silly thing to want to prove until you try a few values for n. We observe the values for $n = 1$ to 7 are $41, 43, 47, 53, 61, 71, 83$ respectively. So far we have gotten only primes. You might be tempted to conjecture, "For all positive integers n, $n^2 - n + 41$ is prime."

If you wanted to prove this, you would need to use a direct proof, a proof by contrapositive, or another style of proof, but certainly it is not enough to give even 7 examples. In fact, we can prove this conjecture is false by proving its negation: "There is a positive integer n such that $n^2 - n + 41$ is not prime." Since this is an existential statement, it suffices to show that there does indeed exist such a number.

In fact, we can check that $n = 41$ will give 41^2, which is certainly not prime. You might say that this is a counterexample to the conjecture that $n^2 - n + 41$ is always prime. Since so many statements in mathematics are universal, making their negations existential, we can often prove that a statement is false (if it is) by providing a counterexample.

1.5 Induction

Perhaps this is the most important proof technique that we will discuss today, since it shows up repeatedly throughout the topics you will study in computer science. Let us begin with some intuition.

1.5.1 Intuition for induction

Consider a planet X, where the following rule holds:

"If it rains one day, it also rains the next day"

Scenario: You land on planet X and it rains on the day you arrive. What can you conclude?

1. It will rain tomorrow on planet X.
2. It has rained every day, till today, on planet X.
3. It rained yesterday on planet X.
4. On planet X, it will rain every day from now on.

Answer: you can legitimately conclude (1) and in fact (4). Planet X is not particularly habitable: either it will never rain, or it will start raining and never stop!

Why? Well we can reason as follows: we see it rained today. By the inductive hypothesis (this is the rule that if it rains on a given day, it will rain on the next day as well), it will rain tomorrow. But now we know it will rain tomorrow, so we can use the rule to say it will definitely rain two days from now...and so on. You can visualize this as a climbing a ladder. The rule says if we are at the i-th step, then we can get to the $(i+1)$-th step. So if we can reach the very first step of the ladder, this means we can keep climbing the ladder, and can reach any step of teh ladder, no matter how high.

Induction is a mathematical strategy for proving that a statement is true for all large n. It goes as follows

- First prove the statement for a small size. **(Base case)**
- Now prove the statement for size n, assuming that it's true for size $n-1$. **(Inductive step)**

1.5.2 A more formal description of induction

We can formalise the idea above as follows. Suppose we wish to prove a statement of the form: $\forall n \in \mathbb{N}, P(n)$.

- First prove that $P(1)$ is true.
- Prove that if $P(m)$ is true, then so is $P(m+1)$.

This proves that $P(n)$ is true for all natural numbers. Note that this is intuitive, but does not follow from any other rules of logic we have discussed. Formally speaking the fact that induction works is another axiom we have to assume in order to reason. For example it is included as an axiom in most axiomatic definitions of the natural numbers. Note that there is nothing special about 1; we could have started at any other number and used induction to prove the statement for all natural numbers from that number onwards.

Theorem 1. *For any natural number n,*

$$1 + 2 + \cdots + (n-1) + n = \frac{n(n+1)}{2}$$

Proof. For $n = 1$, the formula holds. Assume the formula is true for $n = m$. We will now prove it for $n = m + 1$.

$$\begin{aligned}
1 + 2 + \cdots + m + (m+1) &= (1 + 2 + \cdots + (m-1) + m) + m \\
&= \frac{m(m+1)}{2} + (m+1) \\
&= (m+1) \cdot \left(\frac{m}{2} + 1\right) \\
&= \frac{(m+1)(m+2)}{2}
\end{aligned}$$

□

Let's see another example:

Proposition 6. *For all natural numbers n n,* $\log_2 n < n$

Proof. Recall $log_2 x = y$ precisely when $x = 2^y$. For $n = 1$, $log_2 1 = 0 < 1$ so the inequality holds. Assume the inequality for $n = m - 1$. Now we want to prove it for $n = m$.

$$\begin{aligned}\log_2 m &= \log_2(m \cdot \frac{m-1}{m-1})\\ &= \log_2(m-1) + \log_2(\frac{m}{m-1})\\ &= \log_2(m-1) + \log_2(1 + \frac{1}{m-1})\\ &< m - 1 + \log_2(1 + \frac{1}{m-1})\\ &\leq m - 1 + \log_2(1+1) \qquad \text{since } m \geq 2\\ &= m - 1 + \log_2(2)\\ &= m - 1 + 1\\ &= m\end{aligned}$$

□

1.5.3 Strong induction

To do an inductive proof, we are not actually limited to assuming that $P(n-1)$ is true in order to prove $P(n)$. The idea can be extended. Suppose $P(1)$ is true. If we know $P(k)$ is true for all $k < n$ and use this to prove that $P(n)$ is true, then we can carry on this process, using that $P(k)$ is now known to be true for all $k < n+1$ in order to prove it for $n+1$ and so on; thus we can conclude that we have proved the statement for all natural numbers. In general, for the inductive step you can use any subset of $P(i) : i \in 1, 2, \ldots m$ to prove $P(m+1)$.

Proposition 7. *For all $n \in \mathbb{N}$, define a_n as follows*

$$a_n = 2a_{n-1} - a_{n-2}$$

and $a_1 = 3$,$a_2 = 5$. Prove that $a_n = 2n + 1$

Proof. Check the formula for $n = 1$ and 2 and verify it is correct. Assume the formula is true for $n = m - 1$ and $n = m - 2$. We now prove it for a_m:

$$\begin{aligned}a_m &= 2a_{m-1} - a_{m-2}\\ &= 2(2(m-1)+1) - (2(m-2)+1)\\ &= 2(2m-1) - (2m-3)\\ &= 4m - 2 - 2m + 3\\ &= 2m + 1\end{aligned}$$

This concludes the proof. □

Notice that we sometimes require multiple base cases when using strong induction. For example suppose I show that if $P(n-2)$ and $P(n-1)$ are true, then so is $P(n)$. Then I need to show $P(n)$ for two consecutive numbers as base cases.

1.5.4 Strengthening the inductive hypothesis

Sometimes it is hard to assume the statement $P(n)$ and prove $P(n+1)$. However, somewhat unintuitively, you might find it much easier to prove something stronger than what you actually want to prove. This is because doing so gives you a stronger inductive hypothesis to work with. For example suppose I want to prove that the sum of the first n odd numbers is a perfect square. It seems a little unclear how we might use induction. But instead, it is straightforward to prove something stronger: that the sum of the first n odd numbers is not just some perfect square, but in fact it is exactly n^2.

Proposition 8.

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

Proof. For n=1, the formula holds. Suppose it is true for $n = m$. We shall now prove it for $n = m+1$

$$1 + 3 + 5 + \cdots + (2m + 1) + (2(m + 1) - 1) = m^2 + (2(m + 1) - 1) = m^2 + 2m + 1 = (m + 1)^2$$

This concludes the proof. □

You will see another example of this in the homework, where you are asked to prove that, for any natural number n:

$$1 + \frac{1}{2^2} + \frac{1}{3^2} \cdots + \frac{1}{n^2} < 2$$

2 False inductive proof

Look at the false proof in the handout provided and try to state precisely why the induction fails.

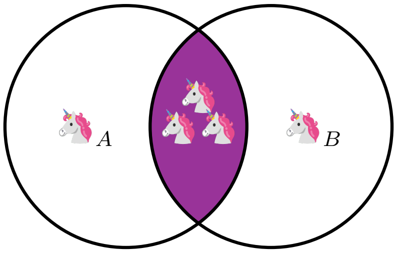

Figure 1: Horses A and B, with all the rest of the horses lying in the violet region common to both the sets.

Claim: For all $n \in \mathbb{N}$, and any set of n horses, all horses in the set have the same color.

1. Base Case ($n = 1$): If there is just one horse in the set, obviously all horses have the same color.

2. Inductive Step: Suppose the induction hypothesis holds for all $1, 2, \dots, n$. Our goal is to prove the statement for sets of $n + 1$ horses. So take any such set. Now exclude one horse, call this horse A, and look at the set of n remaining horses. By the induction hypothesis, they all have the same color. Now exclude a different horse, call it B, and look at the set of n remaining horses, which includes horse A. Then, all horses in this set must also have the same color. This implies that A and B also have the same color. Hence, we obtain that all $n + 1$ horses in our set have the same color, "proving" the claim.

We know that the base case is true. The issue is in going from $n = 1$ to $n = 2$. Let us try to perform the inductive step in this case. The inductive step critically relies on the intersection of the two sets, as shown in Figure 1 is non-empty. However, when $n = 2$ (i.e., applying induction step for $n = 1$), this intersection is indeed empty. There are exactly two horses, A, B. Separating A, gets us that B is a certain color. Separating B, gets us that A is a certain color. However, because there is no intersection, we cannot conclude that A and B are the same color.

3 Recursion

Recursion is ubiquitous in computer science. The key idea of recursion is to define a structure in terms of a smaller version of the same structure. Many data types are recursive: for examples lists, trees and heaps. As we will see induction is a powerful tool to prove properties of recursive structures. Let's begin with a famous example: that of the Fibonacci sequence.

This is the sequence of numbers: $1, 1, 2, 3, 5, 8, 13, 21, 34 \ldots$. Each number in this sequence is the sum of the previous two numbers. Fibonacci numbers show up in a huge number of varied contexts: from architecture to botany. Let's look at a recursive definition. The n-th Fibonacci number, F_n, is defined by

$$F_n = F_{n-1} + F_{n-2}$$

where $F_1 = F_2 = 1$. Note that since we are defining the n-th Fibonacci number in terms of the previous two, we had to state the first two Fibonacci numbers explicitly. This is exactly parallel to the base cases in induction; once we defined the first two Fibonacci numbers, and said what the n-th Fibonacci number is terms of the previous two, we have defined the Fibonacci numbers.

The Fibonacci numbers have lots of amazing mathematical properties. Today let's prove one such simple property: an explicit formula for the um of the squares of the first n Fibonacci numbers. We will do the proof by induction, to illustrate how induction goes really well with proving properties of recursively defined objects.

Theorem 2.

$$F_1^2 + F_2^2 + \cdots + F_n^2 = F_n \times F_{n+1}$$

Proof. Check the base cases, $n = 1$ and $n = 2$:

$$F_1^2 = 1 \times 1 = F_1 \times F_2$$

$$F_1^2 + F_2^2 = 1 \times 1 + 1 \times 1 = 2 = F_2 \times F_3$$

Let $P(k)$ be the claim

$$F_1^2 + F_2^2 + \cdots + F_k^2 = F_k \times F_{k+1}$$

Assume the claim for all k up to m. We will now prove $P(m+1)$

$$\begin{aligned}
F_1^2 + F_2^2 + \cdots + F_{m+1}^2 &= (F_1^2 + F_2^2 + \cdots + F_m^2) + F_{m+1}^2 \\
&= F_m \times F_{m+1} + F_{m+1}^2 \\
&= F_{m+1} \times (F_m + F_{m+1}) \\
&= F_m \times F_{m+2}
\end{aligned}$$

By induction, this concludes the proof.

□

Of course, one dissatisfying thing is that induction doesn't help us guess this property is true or tell us in some intuitive way why it should be true, but given the formula, we could at least prove that it is correct.

4 Structural induction

Structural induction is a proof methodology similar to mathematical induction, only instead of working in the domain of natural numbers, it works in the domain of such recursively defined structures. Such structures show up all the time in computer science: for example lists, arrays, trees and so on. It is terrifically useful for proving properties of such structures. You will see this technique many times when you have to reason about these structure.

The basic idea is the same. We are trying to prove a statement about a recursively defined structure. That is a structure that is defined in terms of smaller versions of the same structure. So we first prove the statement for a fixed small size structure. Next we show that if the desired property is true for the smaller structures, it will be true for the larger structure as well. this let's us conclude that the property is true for all such structures. Let's see this with the example structure of a binary tree.

A binary tree consists of nodes and pointers between them. It is defined as follows:

- Either an empty node.
- Or a root node with an edge pointing to a left child node, that is the root of another binary tree and an edge pointing to a right child node, that is the root of another binary tree.

Proposition 9. *In any binary tree, the number of nodes is exactly one more than the number of edges.*

Proof. Base case: For the single node binary tree, the number of nodes is 1 and the number of edges is 0.

Consider a binary tree. It has a root with two edges going to a left sub-tree and a right subtree. Left the left subtree have v_l nodes and e_l edges and similarly the right subtree have v_r nodes and e_r edges. Then, we can inductively assume the property for these smaller subtrees: so $v_l = e_l + 1$, and $v_r = e_r + 1$. Let v and e be the number of vertices and edges of the overall binary tree. Note that $v = v_l + v_r + 1$ since all vertices in the subtrees are vertcies of the tree and wehave an additional root vertex. Similarly note that $e = e_l + e_r + 2$. Then

$$\begin{aligned} v &= v_l + v_r + 1 \\ &= (e_l + 1) + (e_r + 1) + 1 \\ &= (e_l + e_r + 2) + 1 \\ &= e + 1 \end{aligned}$$

This completes the proof.

□

Excercise 2. *The height of a binary tree is the longest path length from the root of the tree to a node who has no child nodes (also called a leaf). Argue that a binary tree of height h can have at most $2^{h+1} - 1$ nodes.*

5 Some interesting proof techniques

We discussed some of the common proof templates at the beginning of class today. We will now look at some more interesting techniques to prove statements. These are not so much templates of how to do a proof but rather should be viewed as tools that can sometimes be useful to proving things. They are all related to proofs by mathematical induction. Throughout the course you will learn many such tools and will get more practice using them.

5.1 Invariance

This technique comes up quite a lot when reasoning about code. The idea is roughly that when we are analyzing a process that seems complex and hard to keep track of, we can try to find some simpler property that is true at the beginning of the process and remains preserved through every step of the process. Then it will remain true at the end of the process as well. This argument is in fact an inductive argument. Let $P(t)$ be the statement that at step t the invariant property I is true.

- Base Case: check that at step 1 the invariant property I is true, i.e., that $P(1)$ is true.
- Inductive Step: Prove that if the invariant is true at step t, it will also be true at step $t+1$, i.e., $P(t) \implies P(t+1)$.
- If the process ends at step T, conclude $P(T)$ is true.

In general, even though we call I the invariant, it might depend in some way on the time step t, the idea is just that it is some property that holds at every time step.

One way this is used is to reason about loops. A loop might be doing something very complex with a bunch of variables, but if we can find some statement that holds true at the start of the loop, and any arbitrary iteration of the loop has the feature that if the property was true at the start of the iteration, it will be true at the end of that iteration, then we know the property holds when the loop terminates. Let's see a simple example. What is the output of the following? And how can we prove it?

```
x=100;
y=0;
while (x>0){
   x=x-1;
   y=y+1;
}
print(y);
```

We can try to run through a few iterations and because the example is simple, the pattern might become quite obvious. Or we could look at the loop and notice that iterations of the loop increase y by 1 and decrease x by 1, but they don't change the sum $x+y$. Consider the property $x+y = 100$. It is true at the beginning of the loop since $x = 100$ and $y = 0$. If it is true at the beginning of an iteration, it will also be true at the end of the iteration. When the loop terminates $x = 0$. Thus $y = 100$.

In general loops can be much more complex, but finding a useful loop invariant that remains unchanged across iterations can be very helpful in proving things about the loop's behaviour. Let us now look at another example.

A bag contains 99 red marbles and 99 blue marbles. Taking two marbles out of the bag, you:

- put a red marble in the bag if the two marbles you drew are the same color (both red or both blue), and
- put a blue marble in the bag if the two marbles you drew are different colors.

Repeat this step (reducing the number of marbles in the bag by one each time) until only one marble is left in the bag. What is the color of that marble?

Proposition 10. *At the end of the process described above, you will end up with a blue marble.*

Proof. The process is specified in a slightly roundabout way. The thing to notice is that in any step ultimately only one of three things can happen:

- If two reds were taken out, then we put a red marble back in. *So effectively we removed one red marble.*
- If two blues were taken out, then we put a red marble back in. *So effectively we removed two blue marbles and added a red marble.*
- If one red and one blue were taken out, we put the blue one back. *So effectively we removed one red marble.*

Notice that every time we either remove one red, or we add a red and remove two blues. But crucially, the number of blue marbles stays the same or goes down by 2 at every step. Since we started with an odd number of blue marbles and *the number of blue marbles in the bag remains odd at all times.* This is our invariant. So when there is just one marble left it must be blue since there are still an odd number of blue marbles in the bag at that time. □

As you might have noticed, the hard part in invariance based proofs often is coming up with the "right" invariant to consider.

Excercise 3. *Consider a chessboard (*8×8 *grid) with two opposite corners removed. Show that this board cannot be covered completely and exactly with non-overlapping* 2×1 *dominoes.*

Hint: imagine the squares being colored in a checkerboard pattern. Then the opposite corners have the same color. But each domino must cover two squares of different color.

5.2 The well ordering principle

The well-ordering principle is a property of the positive integers which is equivalent to the statement of the principle of mathematical induction. Every nonempty set S of natural numbers contains a least element; there is some natural number a in S such that $\forall b \in s, a \leq b$. Many constructions of the natural numbers take this as an axiom (something that is true by definition). It is useful in proofs of properties of the natural numbers, including in Fermat's method of infinite descent that we will see soon.

An equivalent statement to the well-ordering principle is as follows:

> There does not exist any infinitely long sequence of strictly decreasing natural numbers.

Notice that the principle applies to some sets (like natural numbers), but not all sets. An ordered set is said to be well-ordered if each and every nonempty subset has a smallest or least element. There are plenty of sets that are not well ordered.

Excercise 4. *Describe a set, and an ordering of it's elements, that is not well ordered.*

Suppose you want to prove: $\forall n \in \mathbb{N}, P(n)$.The way proofs using the well ordering principle generally go is as follows.

- Define a set S which is the set of all natural numbers n where $P(n)$ is false.
- Suppose this set was not empty.
- Then S has a smallest element, a, by well-ordering.
- Derive a contradiction from this fact, often by starting with this smallest element a in S and constructing another number b for which $P(b)$ is false that is smaller than a. But b would also be in S so a could not have been the smallest element of S. This is a contradiction.

- So S is empty. But this is precisely what we want to prove.

Well-ordering, by using the above template, can be used to prove statements about some very concrete things

Proposition 11. *For all natural numbers n, $1+2+3+\cdots+n = \frac{n(n+1)}{2}$.*

Proof. Let S be the set of natural numbers where the formula does not hold. Suppose S is not empty. Let a be the smallest element of S. The formula holds for $n = 1$, so a is not 1. That means $a-1$ is also a natural number. Suppose the formula applies for $n = (a-1)$. Thus:

$$1+2+3+\ldots+(a-1) = \frac{(a-1)a}{2}.$$

But now if we add a to both sides:

$$1+2+3+\ldots+(a-1)+a = \frac{(a-1)a}{2} + a = \frac{a^2-a+2a}{2} = \frac{a^2+a}{2} = \frac{a(a+1)}{2}$$

We just assumed the formula holds for $(a-1)$ and showed it works for a. So the formula is false for $(a-1)$, which is a smaller natural number than a. Contradiction. So the set of counter examples to the proposition is empty. This proves the claim. □

5.3 Infinite descent

This is a technique attributed to Pierre de Fermat for stating it explicitly, though the idea had been used before him by others. It makes use of the well ordering principle. Suppose we want to prove a statement like there does not exist any natural number n, satisfying $P(n)$. The typical proof idea is as follows.

- Suppose there did exist a natural number n such that $P(n)$ holds.
- Use this to prove that a strictly smaller natural number $m < n$ also has this property that $P(n)$ holds.
- The two steps above can be repeated to get a smaller natural number where the property P holds, and so on ad infinitum, producing an infinitely long decreasing sequence of natural numbers where P holds.
- By the well-ordering principle, such a sequence can't exist. Contradiction.
- Thus, $P(n)$ cannot be true for any natural number.

Excercise 5. *If we want to write the proof from the previous section of the formula for the sum of the first n natural numbers (Proposition 7) in the above format, what should we use as $P(n)$.*

Proposition 12. *$\sqrt{2}$ is irrational, i.e., it cannot be written as a ratio of two integers numbers p and q where $q \neq 0$.*

Proof. Suppose $\sqrt{2}$ is rational, i.e there are natural numbers p and q such that

$$\sqrt{2} = \frac{p}{q}$$

But then

$$2 = \frac{p^2}{q^2}$$

Or, $p^2 = 2q^2$. This means p^2 is even, so p must also be even (we will see why when we study modular arithmetic, but try to convince yourself of this). Since p is even we can write $p = 2r$ for some natural number r. So

$$2q^2 = p^2 = (2r)^2 = 4r^2$$

From which we get $q^2 = 2r^2$. By the same reasoning we used about p^2 being even, we deduce q is even, so we can write $q = 2s$ for some natural number s. But then

$$\sqrt{2} = \frac{p}{q} = \frac{2r}{2s} = \frac{r}{s}$$

where $s < q$. But then we can keep doing this process getting a sequence of representations of $\sqrt{2}$

$$\sqrt{2} = \frac{p}{q} = \frac{r}{s} = \cdots$$

where we have a sequence of smaller and smaller denominators that are all integers. But this is not possible by the well-ordering principle. □

Note that the well-ordering principle and the method of infinite descent can be used with sets that are not the natural numbers, any well ordered set suffices.

5.4 The extremal principle

The extremal principle is a technique that is useful for solving certain mathematical problems, by studying examples with extreme properties. Most often the object or example we look at will have the smallest or largest value, in some sense. This offers a useful starting point from which we can understand the simplified problem.

Proposition 13. *Suppose you have n people in a field such that the distance between each pair is distinct. Each person is each holding a ball. When I blow a whistle they each throw their ball to the person closest to them. Then there is a pair of people who threw their balls at each other.*

Proof. Consider all pairs of people and the distances between them. Then there must be a smallest distance. Consider a pair of people that has that distance between them. They must throw their balls at each other, because for both of them, the other person is the closest person. □

Another common way such proofs go is by contradiction. You assume that the statement you want to prove is not true and consider some set of structures that arises as a result. Now if the structures have a notion of size, (and say they are finite in number) then consider an extreme structure. Let's say you consider the biggest one. Then prove a bigger one must exist. This results in a contradiction. Here is an example.

Proposition 14. *Consider a tournament for a sport where there can be no draws. There are $n > 2$ participants in the tournament and they all play each other exactly once. Each player makes a list by writing down the name of every player they defeated. Then there must be some player P such that for every other player, their name is written on P's list or the list of some player who P defeated. (Note this is the mathematical use of the word or.)*

Proof. Suppose such a player does not exist. Let A be a player with the most wins in the tournament. Such a player must exist (Why?). There is a player B who is not on A's list, so they defeated A. Consider each person that A defeated, B is not on their lists either. So B defeated every single person that A defeated, as well as A himself. So B has more wins than A. Contradiction. □

Theorem 3. *(Sylvester-Gallai) Let n given points in the plane have the property that they are not all on the same line. Then there is a line that passes through exactly two of them.*

This is known as the Sylvester-Gallai theorem. There is a surprising and elegant proof due to Kelly, that uses the extremal principle. Here is a link to Kelly's proof.

6 Constructive vs non-constructive proofs

A constructive proof is one that proves a certain kind of mathematical object exists by constructing the object or providing an algorithm to construct it. However, it is also possible to prove that an object with some specified properties exist, but provide no explicit example nor any way to construct this object.

Proposition 15. *There is some real number x such that $x^3 + 3x - 2 = 0$.*

Proof. Consider the function $f(x) = x^3 + 3x - 2$. $f(1) > 0$ and $f(0) < 0$. At this point you need some calculus to do a formal proof, but intuitively if you plot $f(x)$ vs x you can see that it is above the x-axis at 1 and below the x-axis at 0, so at some point in between it must cross the x-axis. The value of $x \in (0, 1)$ where this happens is a real value that satisfies the equation. However we have not provided any way to find the exact real value. □

This is a relatively simple example and the proposition can be proved by giving an explicit example (i.e. a constructive proof). However, only nonconstructive proofs are known for a lot of substantial mathematical theorems. Proofs by contradiction can also be nonconstructive in the sense that you assume the statement is false and show that this would mean some statement which is known to be true but only has a non-constructive proof, must be false; thus arriving at a contradiction.

7 Afterword: which proof method is best?

It is good to keep in mind that none of these methods is inherently always better than the others, though this can cause heated debate, especially when it comes to non-constructive proofs and proofs by contradiction. Indeed, it is quite hard to tell if two proofs of the same theorem can be formally justified to be “different”. This might sound odd, but we didn’t really define these proof methods all that formally and the methods we discussed today are quite hard to distinguish between in a precise way. This is in fact a deep question in the philosophy of mathematics. But the takeaway is that, at least for our purposes, we will take the view that all the proof methods we discussed produce equally legitimate proofs and you may choose to use whichever you wish depending on their suitability for the statement being proved and your stylistic preference.