Queen's University
School of Computing

CISC 203: Discrete Mathematics for Computing II
Lecture 1: Proof Techniques
Winter 2019

1 Introduction

In 1175, Alain de Lille wrote "*mīlle viae dūcunt hominēs per saecula Rōmam*", or "a thousand roads lead men forever to Rome". You might know this phrase better by its modern formulation, "all roads lead to Rome". This proverb asserts that one can take many different routes and still end up at the same destination.

"All roads lead to Rome" encompasses the spirit of mathematical discovery; not in the sense that the Romans were mathematical prodigies, but in the sense that there is often not just one correct way to arrive at a desired result. For centuries, mathematicians have discovered and rediscovered various results by attacking the problem from various directions.

In this lecture, we will look at a number of techniques to prove mathematical statements. You have likely seen most of these techniques put to use in some of your previous mathematics or computing courses, possibly without even realizing it.

In the examples throughout these notes, we will prove some statements using the proof techniques we learn in each section. In our example proofs, the steps you should perform when using a given technique will be labelled in bold-italics (***like this***). When you write your proofs on assignments or exams, however, you don't need to label each step explicitly.

Finally, we will use two special terms in our examples, so we define those terms here:

Definition 1 (Odd and even numbers)**.** A number $n \in \mathbb{Z}$ is odd if it can be written in the form $n = 2k + 1$ for some $k \in \mathbb{Z}$. A number n is even if it can be written in the form $n = 2k$ for some $k \in \mathbb{Z}$.

2 Direct Proof

Direct proof is, as the name suggests, the most direct way to prove a statement. A direct proof consists of using a series of known results, axioms, or other facts to establish the truth of a statement. Although the method seems straightforward, every other proof technique we will see builds off of direct proof in some way, so it's good to establish the fundamentals first!

2.1 Conditionals

To begin, we will use the direct proof technique on statements of a certain form: "if x, then y". We call such statements **conditionals**, **implications**, or "if-then" statements.

Definition 2 (Direct proof)**.** To prove that a statement y is true given a statement x that is assumed to be true, prove that the statement "if x, then y" is true.

Since we assume x is true, showing that the statement "if x, then y" is true demonstrates that the truth of y must follow from the truth of x. Within an implication, we call x the **antecedent** and we call y the **consequent**.

Remark. The technique of direct proof is related to the *modus ponens* rule of inference. In this rule, if we know that the statements "if x, then y" and "x" are both true, then we conclude that "y" must also be true.

Example 3. Let us prove the following claim using a direct proof.

Claim. If n is an odd integer, then n^2 is an odd integer.

Proof. (***Assume the antecedent is true***) Suppose n is an odd integer.

(***State known facts***) Then $n = 2k + 1$ for some integer k. Squaring both sides, we get

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

(***Conclude the consequent is true***) Let $j = 2k^2 + 2k$. Then $n^2 = 2j + 1$, so n^2 is an odd integer. □

2.2 Biconditionals

Sometimes, we would like to show that two statements x and y are **logically equivalent**; that is, whenever x is true, then y is also true, and vice versa. Showing the logical equivalence of two statements can make the art of proof writing easier; if we need a result x, but we find that proving x directly is difficult, then we can find a statement y that is both logically equivalent to x and easier to prove and continue from there. A statement asserting logical equivalence is called a **biconditional** or, more colloquially, an "if and only if" statement.

At its core, showing logical equivalence is no different from writing two direct proofs and combining them.

Definition 4 (Logical equivalence)**.** To show that two statements x and y are logically equivalent, show that the statements "if x, then y" and "if y, then x" are both true.

We call the statement "if y, then x" the **converse** of the statement "if x, then y".

2.3 Trivial and Vacuous Proofs

There are two special cases of direct proof that depend on the truth values of x and y in the statement "if x, then y".

- If we can prove that y is always true regardless of the truth value of x, then the statement "if x, then y" is always true. This is called a **trivial proof**.
- If we can prove that x is always false regardless of the truth value of y, then the statement "if x, then y" is always true. This is called a **vacuous proof**.

3 Proof by Counterexample

A **proof by counterexample** is different from a direct proof in that, instead of proving the truth of a statement, we are proving the falsehood of a statement. Indeed, the name "proof by counterexample" is a bit misleading, since we are in fact *dis*proving a statement when we use this method. Since all of our other techniques use the word "proof", however, we will stick with its use here.

Definition 5 (Proof by counterexample)**.** To prove that a statement z is false, find a counterexample that invalidates the assumed truth of z.

In the case where our statement is an implication (if x, then y), then a proof by counterexample involves us finding a particular instance where x is true but y is false. We know what happens when this occurs:

x	y	"if x, then y"
T	T	T
T	F	F
F	T	T
F	F	T

When x is true and y is false, the implication is false. Indeed, this is the only scenario where we get this outcome! Therefore, finding a single instance where both x is true and y is false is enough to invalidate the entire statement.

Example 6. Let us disprove the following claim using a proof by counterexample.

Claim. If n is an even integer, then n^2 is an odd integer.

Proof. (***Assume the statement is true***) Let n be an even integer. Then n^2 must be an odd integer.

(***Find an instance where the antecedent is true***) Suppose $n = 2$.

(***Show that, in this instance, the consequent is false***) Then $n^2 = 4$, which is not an odd integer.

(***Conclude the assumption is false***) Therefore, our assumption was incorrect and n^2 cannot be an odd integer. □

Finding counterexamples can often be difficult, so a proof by counterexample shouldn't be your first approach to a problem. Instead, try solving the problem using another strategy, and then exploit any possible weaknesses in your approach where a counterexample might arise.

As an illustration of how difficult finding a counterexample can be, consider the following claim:

Claim. For all natural numbers $n \in \mathbb{N}$,

$$\left\lceil \frac{2}{2^{1/n} - 1} \right\rceil = \left\lfloor \frac{2n}{\log_e(2)} \right\rfloor .$$

Here, $\lceil \cdot \rceil$ denotes the ceiling function (round up to the nearest integer) and $\lfloor \cdot \rfloor$ denotes the floor function (round down to the nearest integer). If you test small values of n such as 1, 2, or 10 as a sanity check, you will see that the claimed equality holds. Even testing larger values, like 1 000 or 1 million, results in the equality still holding. Surely the equality is always true, then? Not so: the smallest value of n for which the equality does not hold is $n = 777\,451\,915\,729\,368$.

4 Proof by Contrapositive

In certain cases, it may be difficult to attack a problem by starting with a known result and deriving the conclusion. Such cases render the technique of direct proof nearly impossible. Fortunately, we don't always have to work in the forward direction, so to speak. We could instead take the desired conclusion and negate it, then show that the negated conclusion requires our known result to be negated in order for the statement to be valid. For instance, if all students in CISC 203 are fuelled by caffeine, then students who are not fuelled by caffeine are not in CISC 203. Manipulating a statement in this way is called **contraposition**, and a proof that uses this technique is called a **proof by contrapositive** or an **indirect proof**.

Definition 7 (Proof by contrapositive)**.** To prove that a statement "if x, then y" is true, prove that the contrapositive statement "if not-y, then not-x" is true.

To see that a statement and its contrapositive are logically equivalent, let's draw a truth table:

x	y	"if x, then y"	"not-x"	"not-y"	"if not-y, then not-x"
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	T	T

In our truth table, the original statement is the third column and the contrapositive is the sixth column. Since these columns contain exactly the same logical values, the two statements are logically equivalent.

Remark. The technique of proof by contrapositive is related to the *modus tollens* rule of inference, also known as denying the consequent. In this rule, if we know that the statements "if x, then y" and "not-y" are both true, then we conclude that "not-x" must also be true.

Be careful not to confuse taking the contrapositive with the logical fallacy of affirming the consequent; given the statement "if x, then y", you cannot always conclude that its converse form "if y, then x" is true.

Contraposition may be useful when trying to show logical equivalence, especially if proving one direction of the logical equivalence is harder than proving the other direction. For instance, if proving the statement "if y, then x" is difficult, you may attempt to prove the statement "if not-x, then not-y" instead. This observation gives rise to three different but equivalent formulations of logical equivalence:

1. "if x, then y" and "if y, then x" are true;
2. "if x, then y" and "if not-x, then not-y" are true; or
3. "if y, then x" and "if not-y, then not-x" are true.

Example 8. Let us prove the following claim using a proof by contrapositive.

Claim. If n is an odd integer, then n^2 is an odd integer.

Proof. (***Assume the negation of the consequent is true***) Suppose n^2 is not an odd integer.

(***State known facts***) Then n^2 must be even. Add n to n^2 to get

$$n^2 + n = n(n + 1).$$

Since n and $(n + 1)$ differ by one, exactly one of these terms must be even and the other odd. From this, we know that $n^2 + n = n(n + 1)$ is even, since the product of an even integer and an odd integer is even.

(***Conclude the negation of the antecedent is true***) Since the sum $n^2 + n$ is even, and since n^2 is an even integer, n is an even integer. □

Note that, in the previous example, we used a couple of facts that we didn't prove explicitly: namely, "the product of an even integer and an odd integer is even" and "the sum of two even integers is even." These particular facts are elementary, so it's okay to use them without proof. However, when writing proofs of your own, you should always take care not to assume too much knowledge on the part of the reader.

5 Proof by Contradiction

While proofs by counterexample are useful when we wish to prove statements false, a **proof by contradiction** allows us to prove the truth of a statement using the same "false assumption" idea. To write a proof by contradiction, we assume that the statement we are given (that we wish to prove is true) is false, and we show that such an assumption leads to an impossible outcome. Since our assumption that the statement was false led to nonsense, we conclude that our assumption was wrong; the statement must have been true.

Definition 9 (Proof by contradiction)**.** To prove that a statement z is true, assume that the statement "not-z" is true, then arrive at a logical contradiction.

We can think of a proof by contradiction as reducing an argument to an absurd (that is, impossible) conclusion. Along this line of thought, we get the Latin phrase for this proof technique: *reductio ad absurdum.*

How can we be sure that this technique works? We can use truth tables to show that direct proofs and proofs by contradiction are logically equivalent.

If we draw a truth table that includes columns for the statement z we wish to prove and some auxiliary statement a, then we add some columns for our assumption "not-z" and our logical contradiction "a and not-a", and finally we write the latter two statements as an implication in the final column, we get the following:

z	a	"not-z"	"a and not-a"	"if (not-z), then (a and not-a)"
T	T	F	F	T
T	F	F	F	T
F	T	T	F	F
F	F	T	F	F

Observe that our first column (which we may call the "direct proof column") and our last column (which we may call the "proof-by-contradiction column") contain exactly the same logical values, so the two statements represented in those columns are logically equivalent. Therefore, proofs by contradiction are just as valid as any other proof technique.

We can adapt the proof-by-contradiction technique specifically to work on implications in the following way: to prove that the statement "if x, then y" is true, we assume that the statements "x" and "not-y" are simultaneously true and continue from there.

Example 10. Let us prove the following claim using a proof by contradiction.

Claim. If n is an odd integer, then n^2 is an odd integer.

Proof. (***Assume the antecedent is true***) Suppose n is an odd integer.

(***Assume the consequent is false***) Further suppose that n^2 is not an odd integer. Then n^2 must be an even integer.

(***State known facts***) Since n is an odd integer, we have $n = 2k + 1$ for some integer k. Squaring both sides, we get

$$n^2 = 2(2k^2 + 2k) + 1.$$

Let $j = 2k^2 + 2k$. Then $n^2 = 2j + 1$, so n^2 is an odd integer.

(***Reach a contradiction***) However, we assumed that n^2 was not an odd integer.

(***Conclude the assumption is false***) Therefore, our assumption was incorrect and n^2 cannot be an even integer. □

6 Proof by Induction

As a child, you probably played with dominoes at some point by setting each domino on end, one in front of the other, and pushing the first domino over to topple each subsequent domino.

Suppose your younger self wanted to prove that all upright dominoes fall over when acted upon by some external force. (You were a rather bright child.) Pushing over one domino with your finger is enough to show that your idea holds for one domino. Furthermore, lining up dominoes one in front of the other, you can show that if one domino in the line falls, it will contact the next domino and push it over, and so on. Indeed, you can construct this setup using however many dominoes you want, so it must therefore work for all dominoes. Little did you know that you were, in fact, acting out an abstraction of our next proof technique: the **proof by induction**.

Proofs by induction are well-suited for showing that a result holds for infinitely many values. Often, these values come from the set of natural numbers $\mathbb{N}$. Instead of writing infinitely many proofs for each individual value, which can get tiring, a proof by induction requires us to prove only two things: the **base case**, which proves the truth of the statement for some small value, and the **inductive case**, which uses an assumption of truth for some arbitrary value to prove truth for the following value.

Definition 11 (Proof by induction)**.** To prove that a statement z is true over the set of natural numbers $\mathbb{N}$,

1. prove that z is true for some base value $n_0 \in \mathbb{N}$ (base case); and
2. assuming that z is true for some arbitrary value $n \in \mathbb{N}$, prove that z must also be true for the subsequent value $n + 1$ (inductive case).

In this section, we will begin by discussing the two principles of mathematical induction. We will then briefly look at another result that is equivalent to mathematical induction. We conclude with a generalization of mathematical induction that applies to structures other than the set of natural numbers.

6.1 Principle of Mathematical Induction

The principle of mathematical induction is the reliable, multipurpose, all-weather tool that we can use with all of our proofs by induction. The principle, as stated here, is essentially a formalized version of the general "proof by induction" approach we defined earlier.

Proposition 12 (Principle of mathematical induction)**.** *Let P be a statement over the set of natural numbers $\mathbb{N}$. If*

1. $P(1)$ is true; and

2. $P(n)$ being true for any $n = k$ implies that $P(n)$ is true for $n = k + 1$,

then P is true for all $n \in \mathbb{N}$.

Note that, although we use $P(1)$ as the base case in our proposition, we could just as easily take 0 or any other value $n_0 \in \mathbb{N}$ to serve as the base case. Our choice of base case depends on the statement we are trying to prove. However, more often than not, taking $P(1)$ to be our base case will suffice.

Arguably, no notes on induction are complete without some variation on the following popular example.

Example 13. Let us prove the following claim using the principle of mathematical induction.

Claim. For all $n \in \mathbb{N}$, $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

Proof. (***State what we have to prove***) Let $P(n)$ be the statement "$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$".

(***Prove the base case***) When $n = 1$, we have

$$\begin{aligned} 1^2 &= \frac{1(1+1)(2(1)+1)}{6} \\ &= \frac{1(2)(3)}{6} \\ &= \frac{6}{6} \\ &= 1. \end{aligned}$$

Therefore, $P(1)$ is true.

(***Assume the inductive hypothesis***) Assume that $P(k)$ is true for some $k \in \mathbb{N}$. That is, assume that $1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$.

(***Prove the inductive case***) We now show that $P(k+1)$ is true. Add $(k+1)^2$ to both sides of the equation to get

$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{k(k+1)(2k+1)}{6} + \frac{6(k+1)^2}{6} \\ &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\ &= \frac{(k+1)\left[k(2k+1) + 6(k+1)\right]}{6} \\ &= \frac{(k+1)(2k^2+7k+6)}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6} \\ &= \frac{(k+1)\left((k+1)+1\right)\left(2(k+1)+1\right)}{6}. \end{aligned}$$

Therefore, $P(k+1)$ is true.

(***Conclude the statement is true***) By the principle of mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$. □

We need not limit ourselves to using induction to prove formulas. Induction is extremely useful for proving all sorts of things, like properties about sequences. This is because we can index the terms of a sequence using natural numbers. We can also prove inequalities and relationships between values. This particular application comes in handy when evaluating measures like function growth rates, since measuring growth rates is fundamental to the study of the analysis of algorithms.

Example 14. Let us prove the following claim using the principle of mathematical induction.

Claim. For all $n \in \mathbb{N}$ where $n \geq 5$, $2^n > n^2$.

Proof. (***State what we have to prove***) Let $P(n)$ be the statement "$2^n > n^2$".

(***Prove the base case***) When $n = 5$, we have $2^5 > 5^2$; that is, $32 > 25$. Therefore, $P(5)$ is true.

(***Assume the inductive hypothesis***) Assume that $P(k)$ is true for some $k \in \mathbb{N}$. That is, assume that $2^k > k^2$.

(***Prove the inductive case***) We now show that $P(k+1)$ is true; that is, we want to show that $2^{k+1} > (k+1)^2$. Observe that $(k+1)^2 = k^2+2k+1$. Since $k \geq 5 > 1$, we have that $k^2+2k+1 < k^2+2k+k = k^2+3k$. Moreover, since $k \geq 5 > 3$, we have that $k^2+3k < k^2+k(k) = 2k^2$. By the induction hypothesis, $2(2^k) > 2k^2$, so $2^{k+1} > (k+1)^2$. Therefore, $P(k+1)$ is true.

(***Conclude the statement is true***) By the principle of mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$ where $n \geq 5$. □

6.2 Strong Principle of Mathematical Induction

For most proofs, we can get by with the regular principle of mathematical induction and we will have no issues. However, certain proofs require the use of multiple assumptions in order to complete our inductive case. Consider, for instance, a proof involving some value $v_n = v_{n-1} \cdot v_{n-2}$. In order to say anything about the inductive case for v_{k+1}, we would need to have assumptions for both v_k and v_{k-1} simply to define v_{k+1}. While we could feasibly prove statements of this type with the regular principle of mathematical induction, there exists an alternative proof technique that uses a stronger inductive case to make multiple assumptions: the appropriately-named **strong principle of mathematical induction**.

Proposition 15 (Strong principle of mathematical induction)**.** *Let P be a statement over the set of natural numbers $\mathbb{N}$. If*

1. *$P(1)$ is true; and*
2. *$P(n)$ being true for all $n \leq k$ implies that $P(n)$ is true for $n = k+1$,*

then P is true for all $n \in \mathbb{N}$.

If the difference between the regular principle and the strong principle is not clear, look closely at the inductive case. In the formulation of the regular principle, we assume $P(n)$ is true for a single value $n = k$. In the formulation of the strong principle, however, we assume $P(n)$ is true for every value n from 1 to k. Although we might not need to use all k assumptions in our proof, we have them available to us, which makes our job much easier.

Note again that we need not always use $P(1)$ as our base case, since our choice of base case is dependent on what we are proving. In fact, we may even require multiple base cases when using strong induction, for reasons explained in the preceding motivation.

As we saw earlier, induction can be used to prove properties about sequences. Perhaps one of the most famous sequences in all of mathematics is the following, named for the Italian mathematician Fibonacci, who wrote about it in the 13th century:

Definition 16 (Fibonacci sequence)**.** The Fibonacci sequence F is the infinite sequence satisfying the following conditions:

1. $F_1 = 1$;
2. $F_2 = 1$; and
3. $F_n = F_{n-1} + F_{n-2}$ for all $n \in \mathbb{N}$ where $n \geq 3$.

The first ten terms of the Fibonacci sequence are 1, 1, 2, 3, 5, 8, 13, 21, 34, and 55. It doesn't seem too obvious how each term F_n grows as n increases, so let's obtain a lower bound on the growth rate of the Fibonacci sequence to make things a bit clearer.

Example 17. Let us prove the following claim using the strong principle of mathematical induction.

Claim. For all $n \in \mathbb{N}$ where $n \geq 3$, $F_n > \alpha^{n-2}$ where $\alpha = \frac{1+\sqrt{5}}{2}$.

Proof. (***State what we have to prove***) Let $P(n)$ be the statement "$F_n > \alpha^{n-2}$".

(***Prove the base cases***) Since F_n is defined in terms of F_{n-1} and F_{n-2}, we require at least two base cases. Since we know that $n \geq 3$, we take our base cases to be $P(3)$ and $P(4)$. When $n = 3$, we have

$$\alpha^{3-2} = \frac{1+\sqrt{5}}{2} < \frac{1+3}{2} = 2 = F_3.$$

When $n = 4$, we have

$$\alpha^{4-2} = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1+2\sqrt{5}+5}{4} = \frac{3+\sqrt{5}}{2} < \frac{3+3}{2} = 3 = F_4.$$

Therefore, both $P(3)$ and $P(4)$ are true.

(***Assume the inductive hypotheses***) Let $k \geq 4$. Assume that $P(k')$ is true for all $k' \in \mathbb{N}$ where $3 \leq k' \leq k$. That is, assume that $F_{k'} > \alpha^{k'-2}$.

(***Prove the inductive case***) We now show that $P(k+1)$ is true; that is, we want to show that $F_{k+1} > \alpha^{k-1}$. Since $F_{k+1} = F_k + F_{k-1}$, we have by our inductive hypotheses that $F_{k+1} > \alpha^{k-2} + \alpha^{k-3}$. But since

$$\begin{aligned}
\alpha^{k-2} + \alpha^{k-3} &= \alpha^{k-3}(\alpha + 1) \\
&= \alpha^{k-3}\left(\frac{1+\sqrt{5}}{2} + 1\right) \\
&= \alpha^{k-3}\left(\frac{3+\sqrt{5}}{2}\right) \\
&= \alpha^{k-3}\alpha^2 \\
&= \alpha^{k-1},
\end{aligned}$$

we get that $F_{k+1} > \alpha^{k-1}$.

(***Conclude the statement is true***) By the strong principle of mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$ where $n \geq 3$. □

At this point, you may think that the strong principle of mathematical induction is more powerful than the regular principle of mathematical induction because we get more inductive hypotheses “for free”. However, using strong induction actually gives us no additional proof-solving power over using regular induction. We won’t prove this result here, and you won’t be expected to prove it, but it is certainly an important fact to know.

Theorem 18. *The strong principle of mathematical induction and the principle of mathematical induction are equivalent.*

6.3 Well-Ordering Principle

Throughout our discussions on induction, we have been relying on an implicit assumption. All along, we have been assuming that there exists some value that we can use in the base case of each of our proofs. We commonly take this base value to be the smallest natural number for which our statement is true. But how can we be sure such a value exists?

We say that a set A is **well-ordered** if there exists a total order $\sqsubset$ on A with the additional property that every subset of A contains a smallest element under that total order. By “smallest element”, we mean an element $x \in A$ such that, for all $y \in A$, $x \sqsubset y$.

Applying the notion of well-ordering to the set of natural numbers $\mathbb{N}$, we get the key result that allows induction to work.

Proposition 19 (Well-ordering principle)**.** *Every nonempty subset of the set of natural numbers* $\mathbb{N}$ *contains a smallest element.*

In other words, the well-ordering principle tells us that $\mathbb{N}$ is a well-ordered set. Note that $\mathbb{N}$ is a special case; if we consider other sets, like $\mathbb{Z}$, we don’t get the same outcome. (Why? If we take the subset of $\mathbb{Z}$ that contains all negative integers, then this subset contains no smallest element. Therefore, $\mathbb{Z}$ is not well-ordered.)

We can use the well-ordering principle as a proof technique similar to induction. In a **proof by well-ordering**, also called a **proof by smallest counterexample**, we follow a method that mixes together elements of contradiction and induction. By assuming that our statement is false (and, thus, that there exists at least one counterexample to our statement) and then assuming that our statement is true for some value just smaller than the smallest counterexample, we can reach a contradiction that makes our assumption incorrect.

Definition 20 (Proof by well-ordering)**.** Let P be a statement over the set of natural numbers $\mathbb{N}$. To prove that P is true:

1. Suppose that P is false, then take $X \subseteq \mathbb{N}$ to be the set of counterexamples for P. By the well-ordering principle, X contains a smallest element x.
2. Prove that $P(0)$ is true; that is, $x \neq 0$.
3. Assume that $P(x-1)$ is true, then prove that this implies $P(x)$ is true, leading to a contradiction.

Note that, just like with induction, you may require a different base case or multiple base cases when proving something using well-ordering.

Earlier, we used induction to prove a lower bound on the growth rate of the Fibonacci sequence. Now, to get a better picture of the growth rate, let's use a proof by well-ordering to obtain an upper bound as well.

Example 21. Let us prove the following claim using a proof by well-ordering.

Claim. For all $n \in \mathbb{N}$ where $n \geq 1$, $F_n \leq 1.7^{n-1}$.

Proof. (***Assume the statement is false***) Let $P(n)$ be the statement "$F_n \leq 1.7^{n-1}$". Suppose P is false, and let $X = \{n \in \mathbb{N} \mid F_n \not\leq 1.7^{n-1}\}$. Since we have assumed P is false, we know that $X \neq \emptyset$. Moreover, by the well-ordering principle, X contains a smallest element x.

(***Prove the base cases***) Since F_n is defined in terms of F_{n-1} and F_{n-2}, we require at least two base cases. The smallest possible values of n are 1 and 2, so we take our base cases to be $P(1)$ and $P(2)$. When $n = 1$, we have $F_1 = 1 \leq 1.7^0$. When $n = 2$, we have $F_2 = 1 \leq 1.7^1$. Therefore, both $P(1)$ and $P(2)$ are true.

(***Assume the hypotheses***) We know from the base cases that $x \geq 3$. Assume that $P(x-1)$ and $P(x-2)$ are true; that is, both $F_{x-1} \leq 1.7^{x-2}$ and $F_{x-2} \leq 1.7^{x-3}$.

(***Reach a contradiction***) We know that $F_x = F_{x-1} + F_{x-2}$. We have by our inductive hypotheses that $F_x \leq 1.7^{x-2} + 1.7^{x-3}$. Moreover,

$$\begin{aligned}1.7^{x-2} + 1.7^{x-3} &= 1.7^{x-3}(1.7+1) \\ &= 1.7^{x-3}(2.7) \\ &< 1.7^{x-3}(1.7^2) = 1.7^{x-1},\end{aligned}$$

so $F_x \leq 1.7^{x-1}$.

(***Conclude the statement is true***) However, we assumed that $F_x \not\leq 1.7^{x-1}$. Therefore, our assumption was incorrect and P is true. □

In Theorem 18, we saw a connection between regular induction and strong induction. We have a similar result involving the well-ordering principle, though this result is arguably far more important: well-ordering allows us to perform induction, and induction relies on the existence of well-ordered sets. Again, we won't prove this result here.

Theorem 22. *The well-ordering principle and the principle of mathematical induction are equivalent.*

6.4 Structural Induction

Structural induction is a generalization of mathematical induction that is particularly applicable to some of the mathematical structures we will see in this course; namely, trees and graphs. Structural induction is well-suited to proving properties of such structures.

In a proof by structural induction, we replace the set of natural numbers with some mathematical structure that can be recursively defined; that is, the structure is made up of smaller substructures that share the same properties as the structure itself. (For example, trees are made up of subtrees, and a subtree is itself a tree so it shares the same properties.) Using this property together with the existence of a minimal instance of the structure, we can define a partial order on the structure. (Again, for example, $t \sqsubset t'$ if t is a subtree of a tree t', and a minimal instance of a tree is the empty tree. We could also consider a tree with one vertex to be a minimal instance, depending on how we define things.)

Proofs by structural induction follow the same base case/inductive case organization.

Proposition 23 (Principle of structural induction)**.** *Let P be a statement over some recursively-defined structure S. If*

1. *$P(b)$ is true for all minimal instances $b \in S$ of the structure; and*
2. *$P(s)$ being true for any instance $s \in S$ and $s \sqsubset s'$ implies that $p(s')$ is true,*

then P is true for all $s \in S$.

Although we won't look at any examples of proofs by structural induction here, this technique will come in handy for our later lectures on trees and graphs, so it's good to become familiar with structural induction before then.