Chapter 3

Induction and the well ordering Principle

insert DI goes here

3.1 The Well Ordering Principle

Every *nonempty* set of *nonnegative integers* has a *smallest* element.

This statement is known as The *Well Ordering Principle*. Do you believe it? Seems sort of obvious, right? But notice how tight it is: it requires a *nonempty* set —it's false for the empty set which has *no* smallest element because it has no

elements at all! And it requires a set of *nonnegative* integers —it's false for the set of *negative* integers and also false for some sets of nonnegative *rationals* —for example, the set of positive rationals. So, the Well Ordering Principle captures something special about the nonnegative integers.

3.1.1 Well Ordering Proofs

While the Well Ordering Principle may seem obvious, it's hard to see offhand why it is useful. But in fact, it provides one of the most important proof rules in discrete mathematics.

In fact, looking back, we took the Well Ordering Principle for granted in proving that $\sqrt{2}$ is irrational. That proof assumed that for any positive integers m and n, the fraction m/n can be written in *lowest terms*, that is, in the form m'/n' where m' and n' are positive integers with no common factors. How do we know this is always possible?

Suppose to the contrary[1] that there were $m, n \in \mathbb{Z}^+$ such that the fraction m/n cannot be written in lowest terms. Now let C be the set of positive integers that are

[1] This means that you are about to see an informal proof by contradiction.

numerators of such fractions. Then $m \in C$, so C is nonempty. Therefore, by Well Ordering, there must be a smallest integer, $m_0 \in C$. So by definition of C, there is an integer $n_0 > 0$ such that

$$\text{the fraction } \frac{m_0}{n_0} \text{ cannot be written in lowest terms.}$$

This means that m_0 and n_0 must have a common factor, $p > 1$. But

$$\frac{m_0/p}{n_0/p} = \frac{m_0}{n_0},$$

so any way of expressing the left hand fraction in lowest terms would also work for m_0/n_0, which implies

$$\text{the fraction } \frac{m_0/p}{n_0/p} \text{ cannot be in written in lowest terms either.}$$

So by definition of C, the numerator, m_0/p, is in C. But $m_0/p < m_0$, which contradicts the fact that m_0 is the smallest element of C.

Since the assumption that C is nonempty leads to a contradiction, it follows that C must be empty. That is, that there are no numerators of fractions that can't be written in lowest terms, and hence there are no such fractions at all.

We've been using the Well Ordering Principle on the sly from early on!

3.1.2 Template for Well Ordering Proofs

More generally, there is a standard way to use Well Ordering to prove that some property, $P(n)$ holds for every nonnegative integer, n. Here is a standard way to organize such a well ordering proof:

more generally, to

To prove that "$P(n)$ is true for all $n \in \mathbb{N}$" using the Well Ordering Principle, you can take the following steps:

- Define the set, C, of *counterexamples* to P being true. Namely, define[a]

$$C ::= \{n \in \mathbb{N} \mid P(n) \text{ is false}\}.$$

- use a proof by contradiction and assume that C is nonempty.

- By the Well Ordering Principle, there will be a smallest element, n, in C.

- Reach a contradiction (somehow) —often by showing how to use n to find another member of C that is smaller than n. (This is the open-ended part of the proof task.)

- Conclude that C must be empty, that is, no counterexamples exist. QED

[a]The notation $\{n \mid P(n)\}$ means "the set of all elements n, for which $P(n)$ is true.

Take out of box and use bullets

is false

false.

3.1.3 Problems

Class Problems

Homework Problems

3.1.3

3.1.4 Summing the Integers Examples

Let's use this this template to prove

Theorem.

$$1 + 2 + 3 + \cdots + n = n(n+1)/2 \tag{3.1}$$

for all nonnegative integers, n.

First, we better address of a couple of ambiguous special cases before they trip us up:

- If $n = 1$, then there is only one term in the summation, and so $1+2+3+\cdots+n$ is just the term 1. Don't be misled by the appearance of 2 and 3 and the suggestion that 1 and n are distinct terms!

- If $n \leq 0$, then there are no terms at all in the summation. By convention, the

sum in this case is 0.

So while the dots notation is convenient, you have to watch out for these special cases where the notation is misleading! (In fact, whenever you see the dots, you should be on the lookout to be sure you understand the pattern, watching out for the beginning and the end.)

We could have eliminated the need for guessing by rewriting the left side of (3.1) with *summation notation*:

$$\sum_{i=1}^{n} i \qquad \text{or} \qquad \sum_{1 \le i \le n} i.$$

Both of these expressions denote the sum of all values taken by the expression to the right of the sigma as the variable, i, ranges from 1 to n. Both expressions make it clear what (3.1) means when $n = 1$. The second expression makes it clear that when $n = 0$, there are no terms in the sum, though you still have to know the convention that a sum of no numbers equals 0 (the *product* of no numbers is 1, by the way).

OK, back to the proof:

and use of the well ordering Principle.

Proof. By contradiction. Assume that the theorem is *false*. Then, some nonnegative integers serve as *counterexamples* to it. Let's collect them in a set:

$$C ::= \left\{ n \in \mathbb{N} \mid 1+2+3+\cdots+n \neq \frac{n(n+1)}{2} \right\}.$$

By our assumption that the theorem admits counterexamples, C is a nonempty set of nonnegative integers. So, by the Well Ordering Principle, C has a minimum element, call it c. That is, c is the *smallest counterexample* to the theorem.

Since c is the smallest counterexample, we know that (3.1) is false for $n = c$ but true for all nonnegative integers $n < c$. But (3.1) is true for $n = 0$, so $c > 0$. This means $c-1$ is a nonnegative integer, and since it is less than c, equation (3.1) is true for $c - 1$. That is,

$$1+2+3+\cdots+(c-1) = \frac{(c-1)c}{2}.$$

But then, adding c to both sides we get

$$1+2+3+\cdots+(c-1)+c = \frac{(c-1)c}{2} + c = \frac{c^2-c+2c}{2} = \frac{c(c+1)}{2},$$

which means that (3.1) does hold for c, after all! This is a contradiction, and we are done. ∎

3.1.5 Problems

Class Problems

3.1.6 Factoring into Primes

We've previously taken for granted the *Prime Factorization Theorem* that every integer greater than one has a unique[1] expression as a product of prime numbers. This is another of those familiar mathematical facts which are not really obvious. We'll prove the uniqueness of prime factorization in a later chapter, but well ordering gives an easy proof that every integer greater than one can be expressed as *some* product of primes.

Theorem 3.1.1. *Every natural number can be factored as a product of primes.*

Proof. The proof is by Well Ordering. Let C be the set of all integers greater than one that cannot be factored as a product of primes. We assume C is not empty and derive a contradiction.

If C is not empty, there is a least element, $n \in C$, by Well Ordering. The n can't

[1] ...unique up to the order in which the prime factors appear

be prime, because a prime by itself is considered a (length one) product of primes and no such products are in C.

So n must be a product of two integers a and b where $1 < a, b < n$. Since a and b are smaller than the smallest element in C, we know that $a, b \notin C$. In other words, a can be written as a product of primes $p_1 p_2 \cdots p_k$ and b as a product of primes $q_1 \cdots q_l$. Therefore, $n = p_1 \cdots p_k q_1 \cdots q_l$ can be written as a product of primes, contradicting the claim that $n \in C$. Our assumption that $C \neq \emptyset$ must therefore be false. ■

3.2 Induction

Induction is by far the most powerful and commonly-used proof technique in discrete mathematics and computer science. In fact, the use of induction is a defining characteristic of *discrete* —as opposed to *continuous* —mathematics. To understand how it works, suppose there is a professor who brings to class a bottomless bag of assorted miniature candy bars. She offers to share the candy in the following way.

First, she lines the students up in order. Next she states two rules:

1. The student at the beginning of the line gets a candy bar.

2. If a student gets a candy bar, then the following student in line also gets a candy bar.

Let's number the students by their order in line, starting the count with 0, as usual in Computer Science. Now we can understand the second rule as a short description of a whole sequence of statements:

- If student 0 gets a candy bar, then student 1 also gets one.
- If student 1 gets a candy bar, then student 2 also gets one.
- If student 2 gets a candy bar, then student 3 also gets one.

$\vdots$

Of course this sequence has a more concise mathematical description:

> If student n gets a candy bar, then student $n+1$ gets a candy bar, for all nonnegative integers n.

So suppose you are student 17. By these rules, are you entitled to a miniature candy bar? Well, student 0 gets a candy bar by the first rule. Therefore, by the second rule, student 1 also gets one, which means student 2 gets one, which means student 3 gets one as well, and so on. By 17 applications of the professor's second rule, you get your candy bar! Of course the rules actually guarantee a candy bar to *every* student, no matter how far back in line they may be.

3.3 Ordinary Induction

The reasoning that led us to conclude every student gets a candy bar is essentially all there is to induction.

The Principle of Induction.

Let $P(n)$ be a predicate. If

- $P(0)$ is true, and
- $P(n)$ IMPLIES $P(n+1)$ for all nonnegative integers, n,

then

- $P(m)$ is true for all nonnegative integers, m.

Since we're going to consider several useful variants of induction in later sections, we'll refer to the induction method described above as *ordinary induction* when we need to distinguish it. Formulated as a proof rule, this would be

Rule. ***Induction Rule***

$$\frac{P(0), \quad \forall n \in \mathbb{N}. P(n) \text{ IMPLIES } P(n+1)}{\forall m \in \mathbb{N}. P(m)}$$

This general induction rule works for the same intuitive reason that all the students get candy bars, and we hope the explanation using candy bars makes it clear

why the soundness of the ordinary induction can be taken for granted. In fact, the rule is so obvious that it's hard to see what more basic principle could be used to justify it.[2] What's not so obvious is how much mileage we get by using it.

3.3.1 Using Ordinary Induction

Ordinary induction often works directly in proving that some statement about nonnegative integers holds for all of them. For example, here is the formula for the sum of the nonnegative integer that we already proved (equation (3.1)) using the Well Ordering Principle:

Theorem 3.3.1. *For all* $n \in \mathbb{N}$,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \tag{3.2}$$

This time, let's use the Induction Principle to prove Theorem 3.3.1.

Suppose that we define predicate $P(n)$ to be the equation (3.2). Recast in terms of this predicate, the theorem claims that $P(n)$ is true for all $n \in \mathbb{N}$. This is great,

[2] But see section 3.4.

because the induction principle lets us reach precisely that conclusion, provided we establish two simpler facts:

- $P(0)$ is true.

- For all $n \in \mathbb{N}$, $P(n)$ IMPLIES $P(n+1)$.

So now our job is reduced to proving these two statements. The first is true because $P(0)$ asserts that a sum of zero terms is equal to $0(0+1)/2 = 0$, which is true by definition. The second statement is more complicated. But remember the basic plan for proving the validity of any implication: *assume* the statement on the left and then *prove* the statement on the right. In this case, we assume $P(n)$ in order to prove $P(n+1)$, which is the equation

$$1 + 2 + 3 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2}. \tag{3.3}$$

These two equations are quite similar; in fact, adding $(n+1)$ to both sides of equa-

tion (3.2) and simplifying the right side gives the equation (3.3):

$$1+2+3+\cdots+n+(n+1) = \frac{n(n+1)}{2} + (n+1)$$

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

Thus, if $P(n)$ is true, then so is $P(n+1)$. This argument is valid for every nonnegative integer n, so this establishes the second fact required by the induction principle. Therefore, the induction principle says that the predicate $P(m)$ is true for all nonnegative integers, m, so the theorem is proved.

3.3.2 A Template for Induction Proofs

The proof of Theorem 3.3.1 was relatively simple, but even the most complicated induction proof follows exactly the same template. There are five components:

1. **State that the proof uses induction.** This immediately conveys the overall structure of the proof, which helps the reader understand your argument.

2. **Define an appropriate predicate $P(n)$.** The eventual conclusion of the induction argument will be that $P(n)$ is true for all nonnegative n. Thus, you

should define the predicate $P(n)$ so that your theorem is equivalent to (or follows from) this conclusion. Often the predicate can be lifted straight from the claim, as in the example above. The predicate $P(n)$ is called the *induction hypothesis*. Sometimes the induction hypothesis will involve several variables, in which case you should indicate which variable serves as n.

3. **Prove that $P(0)$ is true.** This is usually easy, as in the example above. This part of the proof is called the *base case* or *basis step*.

4. **Prove that $P(n)$ implies $P(n+1)$ for every nonnegative integer n.** This is called the *inductive step*. The basic plan is always the same: assume that $P(n)$ is true and then use this assumption to prove that $P(n+1)$ is true. These two statements should be fairly similar, but bridging the gap may require some ingenuity. Whatever argument you give must be valid for every nonnegative integer n, since the goal is to prove the implications $P(0) \rightarrow P(1)$, $P(1) \rightarrow P(2)$, $P(2) \rightarrow P(3)$, etc. all at once.

5. **Invoke induction.** Given these facts, the induction principle allows you to

conclude that $P(n)$ is true for all nonnegative n. This is the logical capstone to the whole argument, but it is so standard that it's usual not to mention it explicitly.

Always be sure to explicitly label the *base case* and *inductive step*. It will make your proofs clearer, and it will decrease the chance that you forget a key step (such as checking the base case).

3.3.3 A Clean Writeup

3.2.4

The proof of Theorem 3.3.1 given above is perfectly valid; however, it contains a lot of extraneous explanation that you won't usually see in induction proofs. The writeup below is closer to what you might see in print and should be prepared to produce yourself.

Proof of Theorem 3.3.1. We use induction. The induction hypothesis, $P(n)$, will be equation (3.2).

Base case: $P(0)$ is true, because both sides of equation (3.2) equal zero when $n = 0$.

Inductive step: Assume that $P(n)$ is true, where n is any nonnegative integer.

Then

$$1+2+3+\cdots+n+(n+1) = \frac{n(n+1)}{2} + (n+1) \quad \text{(by induction hypothesis)}$$

$$= \frac{(n+1)(n+2)}{2} \quad \text{(by simple algebra)}$$

which proves $P(n+1)$.

So it follows by induction that $P(n)$ is true for all nonnegative n. ■

Induction was helpful for *proving the correctness* of this summation formula, but not helpful for *discovering* it in the first place. Tricks and methods for finding such formulas will appear in a later chapter.

be covered in Part III of the text.

3.2.5 A more challenging Example

3.3.4 Courtyard Tiling

During the development of MIT's famous Stata Center, as costs rose further and further beyond budget, and there were some radical fundraising ideas. One rumored plan was to install a big courtyard with dimensions $2^n \times 2^n$ (as shown in Figure 1 for the case where $n = 3$) and to have one

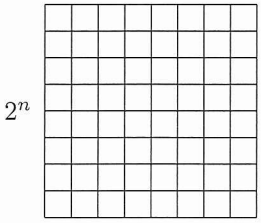


Figure 1: A $2^n \times 2^n$ courtyard for $n = 3$.

continued from prior page

One of the central squares would be occupied by a statue of a wealthy potential donor. Let's call him "Bill". (In the special case $n = 0$, the whole courtyard consists of a single central square; otherwise, there are four central squares.) A complication was that the building's unconventional architect, Frank Gehry, was alleged to require that only special L-shaped tiles be used (shown in Figure 2) for the courtyards.

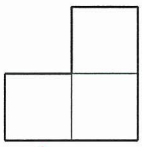


Figure 2: The special L-shaped tile.

It was quickly determined that a courtyard meeting these constraints exists, at least for $n = 2$ (see Figure 3.) But what about for larger values of n? Is

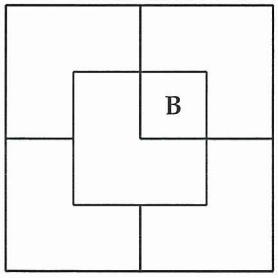


Figure 3: A tiling using L-shaped tiles for $n = 2$ with Bill in a central square.

For larger values of n, is there a way to tile a $2^n \times 2^n$ courtyard with L-shaped tiles and a statue in the center? Let's try to prove that this is so.

Theorem 3.3.2. *For all $n \geq 0$ there exists a tiling of a $2^n \times 2^n$ courtyard with Bill in a central square.*

Proof. (doomed attempt) The proof is by induction. Let $P(n)$ be the proposition that there exists a tiling of a $2^n \times 2^n$ courtyard with Bill in the center.

Base case: $P(0)$ is true because Bill fills the whole courtyard.

Inductive step: Assume that there is a tiling of a $2^n \times 2^n$ courtyard with Bill in the center for some $n \geq 0$. We must prove that there is a way to tile a $2^{n+1} \times 2^{n+1}$ courtyard with Bill in the center ....

Now we're in trouble! The ability to tile a smaller courtyard with Bill in the center isn't much help in tiling a larger courtyard with Bill in the center. We haven't figured out how to bridge the gap between $P(n)$ and $P(n+1)$.

So if we're going to prove Theorem 3.3.2 by induction, we're going to need some *other* induction hypothesis than simply the statement about n that we're try-

ing to prove.

When this happens, your first fallback should be to look for a *stronger* induction hypothesis; that is, one which implies your previous hypothesis. For example, we could make $P(n)$ the proposition that for *every* location of Bill in a $2^n \times 2^n$ courtyard, there exists a tiling of the remainder.

This advice may sound bizarre: "If you can't prove something, try to prove something grander!" But for induction arguments, this makes sense. In the inductive step, where you have to prove $P(n)$ IMPLIES $P(n+1)$, you're in better shape because you can *assume* $P(n)$, which is now a more powerful statement. Let's see how this plays out in the case of courtyard tiling.

Proof. (successful attempt) The proof is by induction. Let $P(n)$ be the proposition that for every location of Bill in a $2^n \times 2^n$ courtyard, there exists a tiling of the remainder.

Base case: $P(0)$ is true because Bill fills the whole courtyard.

Inductive step: Assume that $P(n)$ is true for some $n \geq 0$; that is, for every

location of Bill in a $2^n \times 2^n$ courtyard, there exists a tiling of the remainder. Divide the $2^{n+1} \times 2^{n+1}$ courtyard into four quadrants, each $2^n \times 2^n$. One quadrant contains Bill (**B** in the diagram below). Place a temporary Bill (**X** in the diagram) in each of the three central squares lying outside this quadrant as shown in Figure 4.

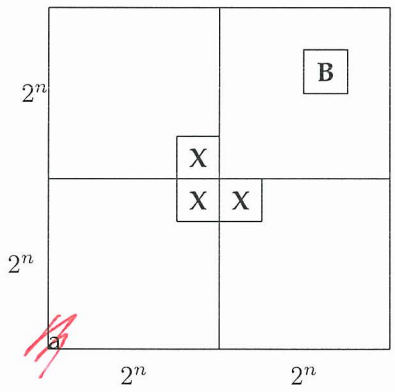


Figure 4: using a stronger inductive hypothesis to prove Theorem 3.3.2.

Now we can tile each of the four quadrants by the induction assumption. Replacing the three temporary Bills with a single L-shaped tile completes the job. This proves that $P(n)$ implies $P(n+1)$ for all $n \geq 0$. The theorem follows as a special case, where we put Bill in a central square. ■

Thus $P(n)$ is true for all $n \in \mathbb{N}$ and the

This proof has two nice properties. First, not only does the argument guarantee that a tiling exists, but also it gives an algorithm for finding such a tiling. Second,

we have a stronger result: if Bill wanted a statue on the edge of the courtyard, away from the pigeons, we could accommodate him!

Strengthening the induction hypothesis is often a good move when an induction proof won't go through. But keep in mind that the stronger assertion must actually be *true*; otherwise, there isn't much hope of constructing a valid proof! Sometimes finding just the right induction hypothesis requires trial, error, and insight. For example, mathematicians spent almost twenty years trying to prove or disprove the conjecture that "Every planar graph is 5-choosable"[3]. Then, in 1994, Carsten Thomassen gave an induction proof simple enough to explain on a napkin. The key turned out to be finding an extremely clever induction hypothesis; with that in hand, completing the argument ~~is~~ was easy!

[3] 5-choosability is a slight generalization of 5-colorability. Although every planar graph is 4-colorable and therefore 5-colorable, not every planar graph is 4-choosable. If this all sounds like nonsense, don't panic. We'll discuss graphs, planarity, and coloring ~~in a later chapter.~~ Part II of the text.

3.2.6

3.3.5 A Faulty Induction Proof

Insert D3 goes here

False Theorem. *All horses are the same color.*

Notice that no n is mentioned in this assertion, so we're going to have to reformulate it in a way that makes an n explicit. In particular, we'll (falsely) prove that

False Theorem 3.3.3. *In every set of $n \geq 1$ horses, all are the same color.*

This a statement about all integers $n \geq 1$ rather ≥ 0, so it's natural to use a slight variation on induction: prove $P(1)$ in the base case and then prove that $P(n)$ implies $P(n+1)$ for all $n \geq 1$ in the inductive step. This is a perfectly valid variant of induction and is *not* the problem with the proof below.

False proof. The proof is by induction on n. The induction hypothesis, $P(n)$, will be

$$\text{In every set of } n \text{ horses, all are the same color.} \tag{3.4}$$

Base case: ($n = 1$). $P(1)$ is true, because in a set of horses of size 1, there's only

one horse, and this horse is definitely the same color as itself.

Inductive step: Assume that $P(n)$ is true for some $n \geq 1$. that is, assume that in every set of n horses, all are the same color. Now consider a set of $n+1$ horses:

$$h_1,\ h_2,\ \ldots,\ h_n,\ h_{n+1}$$

By our assumption, the first n horses are the same color:

$$\underbrace{h_1,\ h_2,\ \ldots,\ h_n}_{\text{same color}},\ h_{n+1}$$

Also by our assumption, the last n horses are the same color:

$$h_1,\ \underbrace{h_2,\ \ldots,\ h_n,\ h_{n+1}}_{\text{same color}}$$

So h_1 is the same color as the remaining horses besides h_{n+1}, and likewise h_{n+1} is the same color as the remaining horses besides h_1. So h_1 and h_{n+1} are the same color. That is, horses $h_1, h_2, \ldots, h_{n+1}$ must all be the same color, and so $P(n+1)$ is true. Thus, $P(n)$ implies $P(n+1)$.

By the principle of induction, $P(n)$ is true for all $n \geq 1$. ■

We've proved something false! Is math broken? Should we all become poets?

No, this proof has a mistake.

INSERT D6 goes here

The error in this argument is in the sentence that begins, "So h_1 and h_{n+1} are the same color." The "..." notation creates the impression that there are some remaining horses besides h_1 and h_{n+1}. However, this is not true when $n = 1$. In that case, the first set is just h_1 and the second is h_2, and there are no remaining horses besides them. So h_1 and h_2 need not be the same color!

This mistake knocks a critical link out of our induction argument. We proved $P(1)$ and we *correctly* proved $P(2) \longrightarrow P(3)$, $P(3) \longrightarrow P(4)$, etc. But we failed to prove $P(1) \longrightarrow P(2)$, and so everything falls apart: we can not conclude that $P(2)$, $P(3)$, etc., are true. And, of course, these propositions are all false; there are horses of a different color.

Students sometimes claim that the mistake in the proof is because $P(n)$ is false for $n \geq 2$, and the proof assumes something false, namely, $P(n)$, in order to prove $P(n+1)$. You should think about how to explain to such a student why this claim would get no credit on a 6.042 exam.

3.3.6 Problems

Class Problems

Homework Problems

3.2.7

make this be a subsection

3.4 Induction versus Well Ordering

The Induction Rule looks nothing like the Well Ordering Principle, but these two proof methods are closely related. In fact, as the examples above suggest, we can take any Well Ordering proof and reformat it into an Induction proof. Conversely, it's equally easy to take any Induction proof and reformat it into a Well Ordering proof.

So what's the difference? Well, sometimes induction proofs are clearer because they resemble recursive procedures that reduce handling an input of size $n+1$ to handling one of size n. On the other hand, Well Ordering proofs sometimes seem more natural, and also come out slightly shorter. The choice of method is really a matter of style and is up to you.

3.3

3.5 Strong Induction

insert DS goes here

Strong Induction is a variation of ordinary induction,

A useful variant of induction is called *strong induction*. Strong Induction and Ordinary Induction are used for exactly the same thing: proving that a predicate $P(n)$ is true for all $n \in \mathbb{N}$.

that comes is very useful for a variety of proofs

new subsection

3.3.1 A Rule for Strong Induction

Principle of Strong Induction. Let $P(n)$ be a predicate. If

- $P(0)$ is true, and
- for all $n \in \mathbb{N}$, $P(0)$, $P(1)$, ..., $P(n)$ *together* imply $P(n+1)$,

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

The only change from the ordinary induction principle is that strong induction allows you to assume more stuff in the inductive step of your proof! In an ordinary induction argument, you assume that $P(n)$ is true and try to prove that $P(n+1)$ is also true. In a strong induction argument, you may assume that $P(0)$, $P(1)$, ..., and $P(n)$ are *all* true when you go to prove $P(n+1)$. These extra assumptions can

only make your job easier. Hence the name: strong induction.

INSERT D9 goes here

~~3.3.1 An Example~~

3.5.1 ~~Products of Primes~~ OK as was

3.3.2 Some Examples

subsubsection w/o number → Products of Primes

As a first example, we'll use strong induction to re-prove Theorem 3.1.1 which we previously proved using Well Ordering.

Lemma 3.5.1. *Every integer greater than 1 is a product of primes.*

Proof. We will prove Lemma 3.5.1 by strong induction, letting the induction hypothesis, $P(n)$, be

$$n \text{ is a product of primes.}$$

So Lemma 3.5.1 will follow if we prove that $P(n)$ holds for all $n \geq 2$.

Base Case: ($n = 2$) $P(2)$ is true because 2 is prime, and so it is a length one product of primes by convention.

Inductive step: Suppose that $n \geq 2$ and that i is a product of primes for every integer i where $2 \leq i < n + 1$. We must show that $P(n + 1)$ holds, namely, that $n + 1$ is also a product of primes. We argue by cases:

If $n+1$ is itself prime, then it is a length one product of primes by convention, and so $P(n+1)$ holds in this case.

Otherwise, $n+1$ is not prime, which by definition means $n+1 = km$ for some integers k, m such that $2 \leq k, m < n+1$. Now by strong induction hypothesis, we know that k is a product of primes. Likewise, m is a product of primes. It follows immediately that $km = n$ is also a product of primes. Therefore, $P(n+1)$ holds in this case as well.

So $P(n+1)$ holds in any case, which completes the proof by strong induction that $P(n)$ holds for all nonnegative integers, n.

■

make it be a subsubsection w/o a number

3.5.2 Making Change

The country Inductia, whose unit of currency is the Strong, has coins worth 3Sg (3 Strongs) and 5Sg. Although the Inductians have some trouble making small change like 4Sg or 7Sg, it turns out that they can collect coins to make change for any number that is at least 8 Strongs.

Strong induction makes this easy to prove for $n+1 \geq 11$, because then $(n+1)-3 \geq 8$, so by strong induction the Inductians can make change for exactly $(n+1)-3$ Strongs, and then they can add a 3Sg coin to get $(n+1)$Sg. So the only thing to do is check that they can make change for all the amounts from 8 to 10Sg, which is not too hard to do.

Here's a detailed writeup using the official format:

Proof. We prove by strong induction that the Inductians can make change for any amount of at least 8Sg. The induction hypothesis, $P(n)$ will be:

If $n \geq 8$, then there is a collection of coins whose value is n Strongs.

Notice that $P(n)$ is an implication. When the hypothesis of an implication is false, we know the whole implication is true. In this situation, the implication is said to be *vacuously* true. So $P(n)$ will be vacuously true whenever $n < 8$.[4]

[4] Another approach that avoids these vacuous cases is to define

$$Q(n) ::= \text{there is a collection of coins whose value is } n + 8\text{Sg},$$

and prove that $Q(n)$ holds for all $n \geq 0$.

We now proceed with the induction proof:

Base case: $P(0)$ is vacuously true.

Inductive step: We assume $P(i)$ holds for all $i \leq n$, and prove that $P(n+1)$ holds. We argue by cases:

Case $(n+1 < 8)$: $P(n+1)$ is vacuously true in this case.

Case $(n+1 = 8)$: $P(8)$ holds because the Inductians can use one 3Sg coin and one 5Sg coins.

Case $(n+1 = 9)$: Use three 3Sg coins.

Case $(n+1 = 10)$: Use two 5Sg coins.

Case $(n+1 \geq 10)$: Then $n \geq (n+1) - 3 \geq 8$, so by the strong induction hypothesis, the Inductians can make change for $(n+1)-3$ Strong. Now by adding a 3Sg coin, they can make change for $(n+1)$Sg.

So in any case, $P(n+1)$ is true, and we conclude by strong induction that for all $n \geq 8$, the Inductians can make change for n Strong. ■

make into a sub sub section without a number

3.5.3 The Stacking Game

Here is another exciting 6.042 game that's surely about to sweep the nation!

You begin with a stack of n boxes. Then you make a sequence of moves. In each move, you divide one stack of boxes into two nonempty stacks. The game ends when you have n stacks, each containing a single box. You earn points for each move; in particular, if you divide one stack of height $a + b$ into two stacks with heights a and b, then you score ab points for that move. Your overall score is the sum of the points that you earn for each move. What strategy should you use to maximize your total score?

As an example, suppose that we begin with a stack of $n = 10$ boxes. Then the game might proceed as follows: shown in Figure A. Can you find a better strategy?

Stack Heights										Score
$\underline{10}$										
5	$\underline{5}$									25 points
$\underline{5}$	3	2								6
$\underline{4}$	3	2	1							4
2	$\underline{3}$	2	1	2						4
$\underline{2}$	2	2	1	2	1					2
1	$\underline{2}$	2	1	2	1	1				1
1	1	$\underline{2}$	1	2	1	1	1			1
1	1	1	1	$\underline{2}$	1	1	1	1		1
1	1	1	1	1	1	1	1	1	1	1
								Total Score	$=$	45 points

Figure A: An example of the stacking game with $n = 10$ boxes. On each line, the underlined stack is divided in the next step.

On each line, the underlined stack is divided in the next step. Can you find a better strategy?

Analyzing the Game

Let's use strong induction to analyze the unstacking game. We'll prove that your score is determined entirely by the number of boxes —your strategy is irrelevant!

Theorem 3.5.2. *Every way of unstacking n blocks gives a score of $n(n-1)/2$ points.*

There are a couple technical points to notice in the proof:

- The template for a strong induction proof is exactly the same as for ordinary induction.

- As with ordinary induction, we have some freedom to adjust indices. In this case, we prove $P(1)$ in the base case and prove that $P(1), \ldots, P(n)$ imply $P(n+1)$ for all $n \geq 1$ in the inductive step.

Proof. The proof is by strong induction. Let $P(n)$ be the proposition that every way of unstacking n blocks gives a score of $n(n-1)/2$.

Base case: If $n = 1$, then there is only one block. No moves are possible, and so the total score for the game is $1(1-1)/2 = 0$. Therefore, $P(1)$ is true.

Inductive step: Now we must show that $P(1), \ldots, P(n)$ imply $P(n+1)$ for all $n \geq 1$. So assume that $P(1), \ldots, P(n)$ are all true and that we have a stack of $n+1$ blocks. The first move must split this stack into substacks with positive sizes a and b where $a + b = n + 1$ and $0 < a, b \leq n$. Now the total score for the game is the sum of points for this first move plus points obtained by unstacking the two resulting substacks:

$$
\begin{aligned}
\text{total score} = {} & (\text{score for 1st move}) \\
& + (\text{score for unstacking } a \text{ blocks}) \\
& + (\text{score for unstacking } b \text{ blocks}) \\
= {} & ab + \frac{a(a-1)}{2} + \frac{b(b-1)}{2} && \text{by } P(a) \text{ and } P(b) \\
= {} & \frac{(a+b)^2 - (a+b)}{2} = \frac{(a+b)((a+b)-1)}{2} \\
= {} & \frac{(n+1)n}{2}
\end{aligned}
$$

This shows that $P(1), P(2), \ldots, P(n)$ imply $P(n+1)$.

Therefore, the claim is true by strong induction. ■

3.3.3 Strong Induction versus Ordinary Induction

Despite the name, strong induction is technically no more powerful than ordinary induction, though it makes some proofs easier to follow. But any theorem that can be proved with strong induction could also be proved with ordinary induction (using a slightly more complicated induction hypothesis). On the other hand, announcing that a proof uses ordinary rather than strong induction highlights the fact that $P(n+1)$ follows directly from $P(n)$, which is generally good to know.

3.5.4 Problems

Class Problems

Insert D1

~~In this chapter~~

Now that you understand the basics of how to prove that a proposition is true, ~~we~~ it is time to equip you with ~~some very powerful tools~~ the most powerful tools we have for establishing truth: ~~induction~~ the Well-Ordering Principle, the Induction Rule, and strong induction. These methods are especially useful when you need to prove that a predicate is true for all natural numbers.

Although the three methods ~~sound~~ look and feel different, it turns out that ~~we will find~~ ~~show at the end of the chapter that~~ ~~that when you look more closely, they~~ they are equivalent in the sense that whatever you can prove using one of the methods, you can also ~~can~~ prove using either of the others. The choice

~~D1~~ D1 (cont) D1-1

of which method to use ~~is up to you~~

depends on whichever seems to be easiest
or most natural
for the problem at hand.

Insert D3

~~When you are~~
If we have done a good job in writing this text, right about now, you should be thinking "Hey, this induction stuff isn't so hard after all – just show P(0) is true and that P(n) ~~←~~ implies P(n+1) for any ~~integer~~ number n." ~~Indeed,~~ ~~it is actually~~ And, you would be right, although sometimes when you start doing induction proofs on your own, you can run into trouble. For example, we will now attempt to ruin your day by using induction to "prove" that all horses are the same color! And just when you thought it was safe to ~~sketch~~ skip class and ~~head to the pub~~ party work on your ~~PSet~~ robot program instead. Bummer!

Insert D6

The first error in this argument is in the sentence that begins "So h_1 is the same color as the remaining horses besides h_{n+1} (i.e., $h_2, \ldots, h_n$)..."

Insert D 8

Strong induction is a variation of ordinary induction that is useful when the predicate $P(n+1)$ naturally depends on $P(a)$ for values of $a < n$. As with ordinary induction, strong induction is used to prove

INSERT D9

Formulated as a proof rule, strong induction ~~would be~~ is:

Rule: Strong Induction Rule

~~$P(0), \forall n \in \mathbb{N}, (P(0) \wedge P(1) \wedge \dots \wedge P(n)) \Rightarrow P(n+1)$~~

$$\frac{P(0),\ \forall n \in \mathbb{N}.\ (P(0) \wedge P(1) \wedge \dots \wedge P(n)) \Rightarrow P(n+1)}{\forall m \in \mathbb{N},\ P(m)}$$

The template for strong induction proofs is identical to the template given in Section 3.2.3 except for two things:

- you should state that your proof is by strong induction, and
- you can assume that $P(0), P(1), \dots, P(n)$ are all true instead of only $P(n)$ during the inductive step.

INSERT

Is strong induction really stronger than ordinary induction? It certainly looks that way. After all, you can assume alot more when proving the induction step. But actually, ~~there is no difference~~ anything that can be proved ~~whatever you can prove~~ with strong induction can also be proved with ordinary induction — you just need to use a "stronger" induction hypothesis.

Which method should you use? ~~Use~~ whichever you find easier. But ~~be sure~~ whichever method you choose, be sure to state the method ~~to be say which method you are using~~ up front so that the reader can understand and more easily verify your proof.

INSERT E1

3.4 Proofs by Invariants

One of the most important uses of induction in computer science involves proving that a program or process preserves one or more desirable properties as it proceeds. A property that is preserved through a series of operations or steps is known as an invariant. Examples of desirable invariants could include properties such as a variable never exceeding a certain value or becoming negative, the altitude of a plane never dropping below 1,000 feet without the wing flaps and landing gear being deployed, and the temperature of a nuclear reactor never exceeding 500 degrees the threshold for a meltdown.

E1-2

We typically use induction to prove ~~To show~~ that ~~a~~ a proposition is an invariant. In particular, we show that the proposition is true at the beginning (this is the base case) and that ~~only~~ if it is true after t steps have been taken, it will also be true after ~~the~~ step $t+1$ (this is the inductive ~~st~~ step). We can then use the induction principle to conclude that the proposition is indeed an invariant, i.e., that it will always hold. ~~So~~

Robot

~~3.4.1 A Simple Example - the Diagonally Moving~~

~~Not surprisingly, we will be seeing~~

~~3.4.1 Establishing that a Proposition is~~

~~Lets~~ ~~an Invariant~~

Invariants are useful in systems that have a start state or configuration

and a well-defined series of steps during which the system can change state.[1] For example, suppose that you have a robot that can walk across diagonals on an infinite 2-dimension grid. The robot starts at position (0,0) and at each step it moves up or down by 1 unit vertically and left or right (but not both) by 1 unit horizontally. To be clear, the robot must move by exactly 1 unit in each dimension during each step since it can only traverse diagonals.

---

[1] Such systems are known as state machines and we will study them in greater depth in Chapter ??.

In this example, the state of the robot ~~after each~~ at any time can be specified by a coordinate pair (x, y) that denotes the robot's position. The start state is $(0, 0)$ since it is given that the robot ~~is specs~~ starts at that position. After the first step, the robot could be in states $(1, 1)$, $(1, -1)$, $(-1, 1)$ or $(-1, -1)$.

~~After two steps, the~~ After two steps, there are ~~even more~~ 9 possible states for the robot, including $(0, 0)$.

Can the robot ever ~~reach~~ ~~position~~ reach position $(1, 0)$? ~~state $(1, 0)$?~~

~~After play.~~

After playing around with the robot for a bit, it will become apparent that the robot will never be able to reach

position (1, 0). ~~although it may take a little effort to~~ This is because the robot can only reach ~~sta~~ positions (x, y) for which x+y is ~~e~~ even, ~~This crucial proposition can be proved to be an observation leads directly to the formulation of a~~ ~~pro~~

This crucial observation quickly leads to the formulation of a predicate

P(t) :: ~~the robot~~ if the robot is in state (x, y) after t steps, then x+y is even,

which ~~can~~ can be prove to be an invariant by induction.

~~T1:~~

Theorem ~~3.5.1~~ The sum of robot's coordinates is always even.

We will prove that P(t) is an invariant by induction.

Proof:

P(0) is true since the robot starts at (0,0) and 0+0 is even.

Assume that P(t) is true for the ~~for an order~~

~~to show P(t) IMPLIES P(t+1)~~.
inductive step. ~~Let~~ Let (x, y) be the position of the robot after t steps. ~~By P~~ Since P(t) is assumed to be true, we know that x+y is even. ~~Case~~ There are four cases ~~to~~ to consider for step t+1 depending on which direction the robot moves.

Case 1: the robot moves to (x+1, y+1). Then ~~the~~ the sum of the coordinates and is x+y+2, which is even, so P(t+1) is true.

Case 2: the robot move to (x+1, ~~y+1~~ y-1). Then the sum of the coordinates is x+y, which is even, and so P(t+1) is true.

Case 3: The robot moves to $(x-1, y+1)$. Then the sum of the coordinates is $x+y$, as with Case 2, and $P(t+1)$ is true.

Case 4: The robot moves to $(x-1, y-1)$. Then the sum of the coordinates is $x+y-2$, which is even, and so $P(t+1)$ is true.

In every case, $P(t+1)$ is true and so we have proved $P(t)$ IMPLIES $P(t+1)$ and so by induction, we know that $P(t)$ is true for all $t \geq 0$.

Corolory 1: The robot can never reach position $(1, 0)$.

Proof: By theorem T1, we know the robot can only reach positions

with coordinates that sum to an even number, and thus, it cannot reach position (1, 0). ∎

Since this was the first time we ~~did a proof by~~ predicate ~~proved~~ proved that a ~~property~~ was an invariant, we were careful to go through all four cases in gory detail. As you become more experienced with such proofs, you will likely become more brief as well. ~~In this case,~~ Indeed, if we were going through this proof again at a later point in the text, we might simply note that ~~the parity of the sum of the coordinates~~ the sum of the coordinates after ~~steps is x+y~~ step b+1 can be only x+y, x+y+2 or x+y-2 and therefore that it is even.

3.4.2 The Invariant Method

In summary, if ~~there~~ you would like to prove that some property ~~ABC~~ NICE holds for every step of a process, then ~~you can~~ it is often helpful to use the following method:

- Define P(t) to be the predicate the NICE holds after ~~the t-th~~ step t. (immediately)
- Show that P(0) is true, namely that NICE holds for the start state.
- Show that ~~P(t) ⇒ P(t+1)~~

  $\forall t \in \mathbb{N}.$ P(t) IMPLIES P(t+1),

  namely, ~~for~~ fix any $t \geq 0$, if NICE holds immediately after step t, ~~,~~ then it must also hold after ~~step~~ the following step.

more Challenging

3.4.3 A ~~Harder~~ Example — The 15-Puzzle

~~In 1874,~~ In the late 19th Century, Noyes Chapman, ~~the~~ a postmaster in Canastota, New York, invented the 15-puzzle[1], ~~a box con~~ which consisted of a 4×4 grid containing 15 numbered blocks ~~labelled 1-15~~ in which the 14-block and the 15-block were out of order. The objective was to move the blocks one at a time into an adjacent ~~op~~ hole in the grid so as to eventually get all 15 blocks into their natural order. A picture of the 15-puzzle is shown in Figure F1 along with the configuration after the 12-block is moved into the hole below. The ~~final~~ desired final configuration

[1] Actually, there is a dispute about who really invented the 15-puzzle. Sam Lloyd, a well known puzzle designer, claimed to be the inventor, but this claim has since been discounted.

is shown in Figure F2.

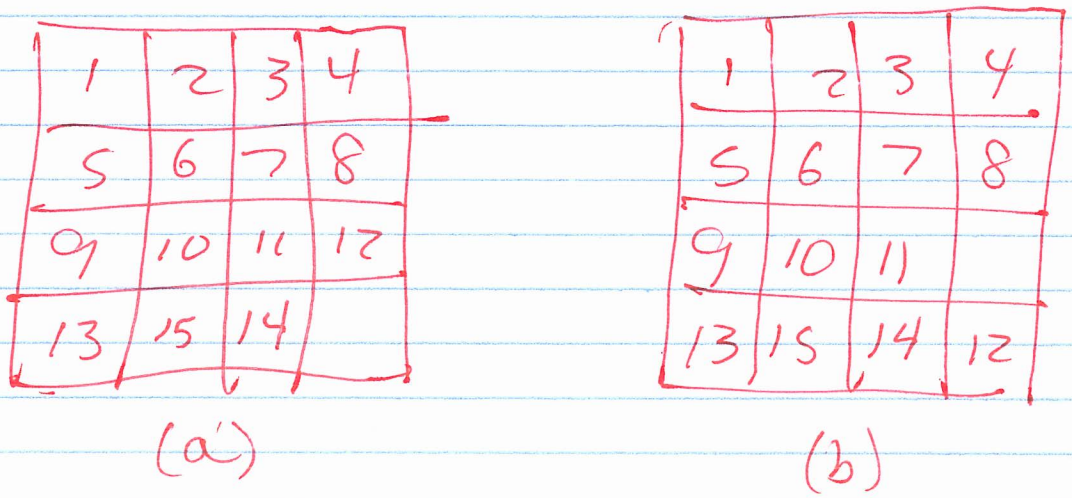


Figure F1 The 15-puzzle in its starting configuration (a) and after the 12-block is moved into the hole below (b).

~~other~~

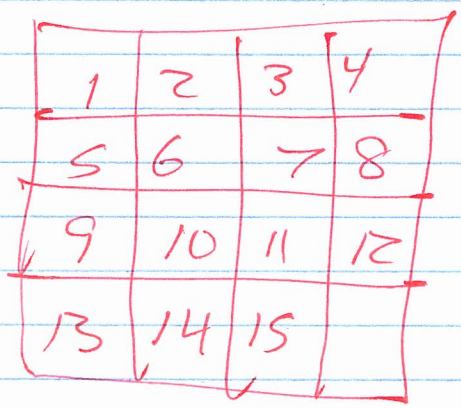


Figure F2: The desired final configuration for the 15-puzzle. Can it be achieved by only moving one block at a time into an adjacent hole?

The 15-puzzle became very popular in North America and Europe and is still sold in game and puzzle shops today. Prizes were offered for its solution, but it is doubtful that they were ever awarded, since it is impossible to get from the configuration in Figure F1 to the configuration in Figure F2 by only moving one block at a time into an adjacent hole. The proof of this fact is a little tricky so we have left it for you to figure out on your own. Instead, we will prove that the analogous task for the much easier 8-puzzle cannot be performed. Both proofs, of course, make use of the invariant method.

Structure long proofs. Long program are usually broken into a heirarchy of smaller procedures. Long proofs are much the same. Facts needed in your proof that are easily stated, but not readily proved are best pulled out and proved in a preliminary lemmas. Also, if you are repeating essentially the same argument over and over, try to capture that argument in a general lemma and then repeatedly cite that instead.

Don't bully. Words such as "clearly" and "obviously" serve no logical function. Rather, they almost always signal an attempt to bully the reader into accepting something which the author is having trouble justifying rigorously. Don't use these words in your own proofs and go on the alert whenever you read one.

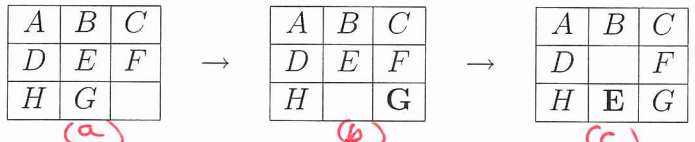
Finish. At some point in a proof, you'll have established all the essential facts you need. Resist the temptation to quit and leave the reader to draw the right conclusions. Instead, tie everything together yourself and explain why the original claim follows.

The analogy between good proofs and good programs extends beyond structure. The same rigorous thinking needed for proofs is essential in the design of critical computer system. When algorithms and protocols only "mostly work" due to reliance on hand-waving arguments, the results can range from problematic to catastrophic. An early example was the Therac 25, a machine that provided radiation therapy to cancer victims, but occasionally killed them with massive overdoses due to a software race condition. More recently, a buggy electronic voting system credited presidential candidate Al Gore with *negative* 16,022 votes in one county. In August 2004, a single faulty command to a computer system used by United and American Airlines grounded the entire fleet of both companies— and all their passengers.

It is a certainty that we'll all one day be at the mercy of critical computer systems designed by you and your classmates. So we really hope that you'll develop the ability to formulate rock-solid logical arguments that a system actually does what you think it does.

2 The 8 Puzzle

Here is a puzzle. There are 8 lettered tiles and a blank square arranged in a 3×3 grid. Any lettered tile adjacent to the blank square can be slid into the blank. For example, a sequence of two moves is illustrated below:



We'll only be considering legal moves in this lecture!

In the leftmost configuration shown above, the G and H tiles are out of order. We can find a way of swapping G and H so that they are in the right order, but then other letters

may be out of order. Can you find a sequence of moves that puts these two letters in the correct order, but returns every other tile to its original position? Some experimentation suggests that the answer is probably "no", so let's try to prove that. and we will prove that is so by finding an invariant (i.e.,

We're going to take an approach that is frequently used in the analysis of software and systems. We'll look for an ***invariant***, a property of the puzzle that is always maintained, no matter how you move the tiles around). If we can then show that putting the G and H tiles in the correct order would violate the invariant, then we can conclude that this is impossible. all the the puzzle cannot be solved.

Let's see how this game plan plays out. Here is the theorem we're trying to prove:

Theorem 1. *No sequence of legal moves transforms the board below on the left into the board below on the right.*

configuration in Figure F4. configuration in Figure F3(a)

A	B	C
D	E	F
H	G	

A	B	C
D	E	F
G	H	

Figure F4: The desired final configuration of the 8-puzzle.

We'll build up a sequence of observations, stated as lemmas. Once we achieve a critical mass, we'll assemble these observations into a complete proof of Theorem 1.

Define a ***row move*** as a move in which a tile slides horizontally and a ***column move*** as one in which a tile slides vertically. Assume that tiles are read top-to-bottom and left-to-right like English text, that is, the *natural order*, defined as follows:

1	2	3
4	5	6
7	8	9

So when we say two tiles are "out of order", we mean that the larger letter precedes the smaller letter in this natural order.

Our difficulty is that one pair of tiles (the G and H) is out of order initially. An immediate observation is that row moves alone are of little value in addressing this problem:

Lemma 2. *A row move does not change the order of the tiles.*

Proof. A row move moves a tile from cell i to cell $i+1$ or vice versa. This tile does not change its order with respect to any other tile. Since no other tile moves, there is no change in the order of any of the other pairs of tiles. □

Let's turn to column moves. This is the more interesting case, since here the order can change. For example, the column move shown below changes the relative order of the pairs (G, H) and (G, E). in Figure F5 changes

A	B	C
D	F	
H	E	G

→

A	B	C
D	F	G
H	E	

Figure F5: An example of a column move in which the G-block G-tile is moved upward into the adjacent hole above. In this case, G changes order with E and H.

E1 -15

Lemma 3. *A column move changes the relative order of exactly two pairs of tiles.*

Proof. Sliding a tile down moves it after the next two tiles in the order. Sliding a tile up moves it before the previous two tiles in the order. Either way, the relative order changes between the moved tile and each of the two it crosses. The relative order between any other pair of tiles does not change. □

These observations suggest that there are limitations on how tiles can be swapped. Some such limitation may lead to the invariant we need. In order to reason about swaps more precisely, let's define a term referring to a pair of items that are out of order:

Definition 1. *A pair of letters L_1 and L_2 is an **inversion** if L_1 precedes L_2 in the alphabet, but L_1 appears after L_2 in the puzzle order.*

For example, in the puzzle below, there are three inversions: (D, F), (E , F) and (G, E).

A	B	C
F	D	G
E	H	

There is exactly one inversion (G,H) in the start state:

A	B	C
D	E	F
H	**G**	

There are no inversions in the end state:

A	B	C
D	E	F
G	**H**	

Let's work out the effects of row and column moves in terms of inversions.

Lemma 4. *During a move, the number of inversions can only increase by 2, decrease by 2 or remain the same.*

Proof. By Lemma 2, a row move does not change the order of the tiles; thus, in particular, a row move does not change the number of inversions.

By Lemma 3, a column move changes the relative order of exactly 2 pairs of tiles. There are three cases: If both pairs were originally in order, then the number of inversions after the move goes up by 2. If both pairs were originally inverted, then the number of inversions after the move goes down by 2. If one pair was originally inverted, and the other was originally in order, then the number of inversions stays the same (since the changing the former pair makes the number of inversions smaller by 1, and changing the latter pair makes the number of inversions larger by 1). □

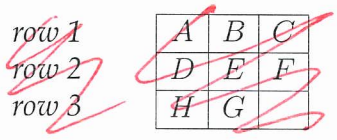
We are almost there. If the number of inversions only change by 2, then what about the parity? That is, the "parity" of a number refers to whether the number is even or odd. For example, 7 and 5 have odd parity, and 18 and 0 have even parity.

Since adding or subtracting 2 from a number does not change the parity, we have the following corollary:

Corollary 5. *Neither a row nor a column move ever changes the parity of the number of inversions.*

Now we can bundle up all these observations and state an *invariant*, that is, a property of the puzzle that never changes, no matter how you slide the tiles around.

Lemma 6. *In every configuration reachable from the position shown below, the* parity of the number of inversions is odd.



Proof. We use induction. Let $P(n)$ be the proposition that after n moves from the above configuration, the parity of the number of inversions is odd.

Base case: After zero moves, exactly one pair of tiles is inverted (H and G), which is an odd number. Therefore, $P(0)$ is true.

Inductive step: Now we must prove that $P(n)$ implies $P(n+1)$ for all $n \geq 0$. So assume that $P(n)$ is true; that is, after n moves the parity of the number of inversions is odd. Consider any sequence of $n+1$ moves $m_1, \ldots, m_{n+1}$. By the induction hypothesis $P(n)$, we know that the parity after moves $m_1, \ldots, m_n$ is odd. By Corollary 5, we know that the parity does not change during m_{n+1}. Therefore, the parity of the number of inversions after moves $m_1, \ldots, m_{n+1}$ is odd, so we have that $P(n+1)$ is true.

Thus, $P(n)$ implies $P(n+1)$ for all $n \geq 0$.

By the principle of induction, $P(n)$ is true for all $n \geq 0$. □

The theorem we originally set out to prove is restated below. With this invariant in hand, the proof is simple.

Theorem. *No sequence of moves transforms the board below on the left into the board below on the right.*

A	B	C
D	E	G
H	**G**	

A	B	C
D	E	F
G	**H**	

Proof. In the target configuration on the right, the total number of inversions is zero, which is even. Therefore, by Lemma 6, the target configuration is unreachable. □

3.5 Problems