Queen's University
School of Computing

CISC 203: Discrete Mathematics for Computing II
Module 5: Proof Methods (Continued)
Fall 2021

This module corresponds to the following sections from your textbook:

22. Induction
23. Recurrence Relations (excluding subsection on Sequences Generated by Polynomials)

1 Proof by Induction

Proof by induction is a more popular alternative to proof by smallest counterexample. In fact, anything that can be proved by smallest counterexample can be proved by induction, and vice-versa.

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 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.

1.1 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.

Theorem 1 (Principle of mathematical induction)**.** *Let A be a set of natural numbers. If*

- *$0 \in A$, and*
- *for every $k \in \mathbb{N}$ where $k \in A$, we also have $k + 1 \in A$,*

then the only way these two conditions can be met is if $A = \mathbb{N}$.

Proof. We prove this by the well-ordering principle.

(***Assume the statement is false***) Suppose that $A \neq \mathbb{N}$. Let $X = \mathbb{N} - A$, i.e., X is the set of natural numbers not in A. It follows from our supposition that that $X \neq \emptyset$. By the well-ordering principle, there must be a smallest natural number $x \in X$.

(***Show that the statement holds for the basis step***) For $k = 0$, we have $k \in A$ since we are given that $0 \in A$ in the first condition. Therefore, $0 \notin X$ and $x \geq 1$.

(***Consider*** $x - 1$) Since $x \geq 1$, we have $x - 1 \geq 0$, which means that $x - 1 \in \mathbb{N}$.

(***Reach a contradiction by showing that the statement is true for*** x) Since x is the smallest natural number not in A, we have $x - 1 \in A$.

The second condition gives us that for any natural number in A, the next larger natural number must also be in A. So if $x - 1 \in A$, it follows that $x \in A$. But this contradicts $x \in X$. $\Rightarrow\Leftarrow$

(***Conclude the statement is true***) We have shown that there can not exist a smallest natural number $x \in X$, and therefore the principle of mathematical induction is true. □

It is worth noting that the Well-Ordering Principle (from the previous module) can be proven by the principle of mathemetical induction as well. In other words, the two principles imply each other.

1.2 Proof by Induction

Using the principle of mathematical induction, we formalize the following proof by induction template.

Definition 2 (Proof by induction)**.** To prove that a statement is true for all $n \in \mathbb{N}$,

1. **Base case:** Verify that the result is true for $n = 0$.
2. **Inductive hypothesis:** Assume that the statement is true for $n = k$.
3. **Inductive step:** Prove that the statement is true for $n = k + 1$.

These steps are logically equivalent to Proof Template 17 (p. 137) in your textbook, which describes the steps using set notation, as we did for defining and proving the principle of mathematical induction in Theorem 1.

Although we use $n = 0$ as the base case, we could just as easily take $n = 1$ 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.

Example 3. Let us prove the following claim using the principle of mathematical induction.

Claim. For all $n \in \mathbb{N}$ where $n \geq 1$,

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

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 4. 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 show that $2^{k+1} > (k+1)^2$.

Observe that $(k+1)^2 = k^2+2k+1$. Since $k \geq 5$ and $5 > 1$, we have that $k^2+2k+1 < k^2+2k+k = k^2+3k$.

Moreover, since $k \geq 5$ and $5 > 3$, we have that $k^2 + 3k < k^2 + k(k) = 2k^2$.

So, since $2k^2 > (k+1)^2$, if we can show that $2^{k+1} > 2k^2$, this would mean that $2^{k+1} > (k+1)^2$.

By our inductive hypothesis, we know that $2(2^k) > 2k^2$, which means that $2^{k+1} > (k+1)^2$. 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 $n \geq 5$. □

Exercise

Prove, using the same technique, that for $n \geq 3$,

$$1 + 2n < 2^n.$$

Exercise

Recall in Module 1 that we proved combinatorically that

$$2^0 + 2^1 + \cdots + 2^{n-1} = 2^n - 1.$$

Now, prove this equation by induction. You may check your work by comparing with the proof for Proposition 22.4 on p. 139 of your textbook.

1.3 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 $v_n = v_{n-1} + v_{n-2}$. 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**.

Theorem 5 (Strong principle of mathematical induction)**.** *Let A be a set of natural numbers. If*

- $0 \in A$*, and*
- *For every $k \in \mathbb{N}$ where $0, 1, 2, \ldots, k \in A$, it must be the case that $k + 1 \in A$,*

then the only way these two conditions can be met is if $A = \mathbb{N}$.

Using the strong principle of mathematical induction, we formalize the following proof by strong induction template.

Definition 6 (Proof by strong induction)**.** To prove that a statement is true for all $n \in \mathbb{N}$,

1. **Base case:** Verify that the result is true for $n = 0$.
2. **Strong inductive hypothesis:** Assume that the statement is true for $n = 0, 1, 2, \ldots, k$.
3. **Inductive step:** Prove that the statement is true for $n = k + 1$.

These steps are logically equivalent to Proof Template 18 (p. 142) in your textbook, which describes the steps using set notation, as we did for defining and proving the strong principle of mathematical induction in Theorem 5.

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 the statement is true for a single value $n = k$. In the formulation of the strong principle, however, we assume the statement is true for every value n from 0 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 $n = 0$ 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.

We demonstrate the strong principle of induction with the following example that shows a lower bound for the Fibonacci number F_n.

Example 7. 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 $F_n > \alpha^{n-2}$.

(***Verify 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

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

When $n = 4$, we have

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

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

(***Assume the strong inductive hypotheses***) Let $k \geq 4$. Assume that $P(n)$ is true for $n = 3, 4, \ldots, k$. That is, assume that $F_n > \alpha^{n-2}$ for $n = 3, 4, \ldots, k$.

(***Prove the inductive case***) We now show that $P(k+1)$ is true; that is, we want to show that $F_{k+1} > \alpha^{k-1}$. By our strong inductive hypothesis, we have $F_k > \alpha^{k-2}$ and $F_{k-1} > \alpha^{k-3}$ (note that without strong induction, we would be able to make the assumption on F_k but not on F_{k-1}).

Since $F_{k+1} = F_k + F_{k-1}$, it follows from above 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 $n \geq 3$. □

Exercise

A sequence a_n is defined recursively by

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 3 \\ a_n &= 2a_{n-1} - a_{n-2}, \text{ for } n \geq 3. \end{aligned}$$

Prove, using strong induction, that $a_n = 2n - 1$ for all $n \in \mathbb{N}$.

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

We conclude with a final example using proof by strong induction.

Example 9. Let us prove the following claim using the strong principle of mathematical induction.

Claim. For each integer $n \geq 8$, there are nonnegative integers a and b such that $n = 3a + 5b$.

Proof. (***State what we have to prove***) Let $P(n)$ be the statement $n = 3a + 5b$ for some nonnegative integers a and b.

(***Verify the base cases***) We have

$$\begin{aligned} 8 &= 3 \cdot 1 + 5 \cdot 1 \\ 9 &= 3 \cdot 3 + 5 \cdot 0 \\ 10 &= 3 \cdot 0 + 5 \cdot 2 \end{aligned}$$

(***Assume the strong inductive hypotheses***) Assume that $P(n)$ is true for $8 \leq n \leq k$.

(***Prove the inductive case***) We now show that $P(k+1)$ is true; that is, we want to show that $k+1 = 3a+5b$ for some nonnegative integers a and b.

We know this is true for $k+1 = 9$ and $k+1 = 10$, so we need to prove the statement for

$$k + 1 \geq 11.$$

It follows from the above inequality that

$$8 \leq (k+1) - 3 < k.$$

By the strong induction hypothesis, we know that the statement is true for $n = 8, 9, 10, \ldots, k$, so we have

$$(k+1) - 3 = 3x + 5y$$

for some nonnegative integers x and y. From this, we obtain that

$$\begin{aligned} k + 1 &= 3x + 3 + 5y \\ &= 3(x+1) + 5y \\ &= 3a + 5b, \end{aligned}$$

where $a = x + 1$ and $b = y$.

(***Conclude the statement is true***) By the strong principle of mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$ where $n \geq 8$. □

Exercise

Using the same technique, prove that for each integer $n \geq 12$, there are nonnegative integers a and b such that $n = 3a + 7b$.

Exercise

Induction and strong induction can also be used to prove the solutions to many interesting geometric problems. Read and understand the proof for Proposition 22.10 on p. 142 in your textbook. Then, clearly state why strong induction is required for this proof (as opposed to just "standard" induction).

2 Recurrence Relations

Let $k \in \mathbb{N}$ be fixed. We want to define for each $n \geq k$ some entity $P(n)$, where $P(n)$ could be, e.g., a number or a set. Based on the induction principle this can be done as follows:

1. Define $P(k)$.
2. Give a rule that tells us how we get $P(n+1)$ when $P(k)$, $P(k+1)$, $\ldots$, $P(n)$ are known.

A definition of the above type is called a *recurrence relation*. In the general form given in Requirement 2 above, $P(n+1)$ can depend on all the previous elements $P(k)$, $P(k+1)$, $\ldots$, $P(n)$. In typical use of recurrence relations the term $P(n+1)$ depends only on a constant number of previous terms.

Definition 10 (Recurrence relation)**.** A recurrence relation is a sequence $P(n)$ where each term of the sequence is either given as an initial term or produced from one or more previous terms using Requirement 2.

Thinking in the other direction, we say that a sequence is a **solution** of a recurrence relation if the terms of the sequence satisfy the recurrence relation. A recurrence relation together with a set of initial terms uniquely defines a sequence, so there exists only one sequence that satisfies a given recurrence relation.

Example 11 (Fibonacci sequence)**.** A well known example of a sequence of numbers defined by a recurrence relation is the *Fibonacci sequence* that we have already encountered previously. The initial numbers are

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

The recurrence relation defining the Fibonacci sequence is

1. $F_0 = 0$ and $F_1 = 1$;
2. $F_{n+1} = F_n + F_{n-1}$, $(n \geq 2)$.

The definition of the Fibonacci numbers gives two base values (F_0 and F_1) and, in the recurrence relation, F_{n+1} depends on the two previous values. Because of this, in inductive proofs of properties of Fibonacci numbers in the base case we need to verify that the property holds for the first two values of n.

Fibonacci numbers satisfy many interesting identities. The below lemma gives two examples. The identities can be proved using induction.

Lemma 12. *1.* $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$ *(*$n \geq 1$*);*

2. $F_{m+n} = F_m F_{n+1} + F_{m-1} F_n$ *(*$n \geq 0$*,* $m \geq 1$*).*

A second example is the binomial coefficients that we have also encountered previously.

Example 13. The binomial coefficients $B_{n,k} = \binom{n}{k}$ have the following properties:

1. $\binom{n}{0} = 1$ for all $n \in \mathbb{N}$;
2. $\binom{n}{n} = 1$ for all $n \in \mathbb{N}$; and
3. $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ for all $1 \leq k \leq n$.

The sequence $B_{n,k}$ is generated by the recurrence relation

$$B_{n,k} = B_{n-1,k} + B_{n-1,k-1},$$

with initial terms $B_{n,0} = 1$ and $B_{n,n} = 1$.

In both of the above examples, we obtain new terms of the sequence recursively by adding together two previous terms of the sequence. We are also given two initial terms for each sequence, which we use to obtain the first recursive term of that sequence. However, it is possible to define recurrence relations that use more than two previous terms. In general, if a recurrence relation produces new terms from k previous terms, we say that the **degree** of the recurrence relation is k. We may also refer to such a recurrence relation as a ***k*th-order** recurrence relation.

Example 14. We can define common functions using recurrence relations. Consider the exponential function 2^n. Each value of 2^n is given by the first-order recurrence relation $a_n = 2 \cdot a_{n-1}$, and the initial term of the recurrence relation is $a_1 = 1$ (where a_1 corresponds to $2^0 = 1$).

Example 15. Each value of the factorial function $n!$ is given by the first-order recurrence relation $b_n = n \cdot b_{n-1}$, and the initial term of the recurrence relation is $b_1 = 1$.

Observe that in Example 14 the recurrence a_n had a coefficient of 2 for all terms, while in Example 15 the recurrence b_n had a coefficient of n for the nth term. We say that a_n is a recurrence relation with **constant coefficients**; that is, coefficients that do not depend on n. The recurrence relation b_n, however, contains the non-constant coefficient n.

Example 16. Consider the recurrence relation $d_n = d_{n-1} + 1$ with initial term $d_1 = 1$. This first-order, constant-coefficient recurrence relation simply produces the sequence of all positive integers.

Example 17. By modifying the Fibonacci recurrence relation to multiply previous terms together, we get a slightly more interesting recurrence relation. Call this recurrence relation $e_n = e_{n-1} \cdot e_{n-2}$, and define the initial terms to be $e_1 = 1$ and $e_2 = 2$. This second-order recurrence relation produces the sequence $1, 2, 2, 4, 8, 32, 256, 8192, \ldots$.

In the recurrence relation e_n, we get new terms by multiplying previous terms instead of adding. If a recurrence relation defines the nth value by a linear function of some previous value, then we say that the recurrence is **linear** (and, thus, the recurrence relation e_n is non-linear, since the nth term is the product of e_{n-1} and e_{n-2}).

2.1 Solving Recurrences

Now that we are familiar with defining recurrence relations, we turn to the converse question: how do we solve recurrence relations? Here, we use the word "solve" in the sense of finding a closed-form equation that is equivalent to the recursively-defined recurrence relation. There exist a number of approaches we can take when solving a recurrence relation, and these approaches range from the simple to more complex ones. Our choice of approach ultimately depends on the recurrence relation we are trying to solve.

To illustrate the simplest method for solving let us consider the so called *Towers of Hanoi problem.*

Example 18 (Towers of Hanoi)**.** We are given n discs of different size placed on three pegs. A disc can slide into any peg. Initially all the discs are placed in the first peg in order of size (thus making a conical shape).

The goal is to move the n discs to the third peg following the rules:

1. only one disc can be moved at a time;
2. at any moment a larger disc cannot be placed on top of a smaller disc.

One can verify that for small values of n the smallest number of moves required will be, respectively,

$$1, 3, 7, 15, 31, 63, 127, \ldots$$

Notice that each term of the sequence $H_n = (1, 3, 7, 15, 31, 63, 127, \ldots)$ seems to be twice the previous term plus one. This suggests that the sequence H_n can be generated by a recurrence $H_n = 2H_{n-1} + 1$. Since we have three pegs, we can model the problem recursively by moving all but the largest disk from the first peg to the second peg, then moving the largest disk to the third peg before placing all of the other disks on the third peg as well.

Lemma 19. *Given n disks, $H_n = 2H_{n-1} + 1$ moves are sufficient to transfer all disks from peg 1 to peg 3, where $H_1 = 1$.*

Proof We begin with all n disks on peg 1. Move the top $n-1$ disks from peg 1 to peg 2. This step requires H_{n-1} moves. Then, move the nth disk (that is, the largest disk) to peg 3. Finish by moving the top $n-1$ disks from peg 2 to peg 3. Altogether, this process uses a total of $2H_{n-1} + 1$ moves. □

You might question whether this bound is also the minimum and, indeed, this bound is the best possible. Roughly, this can be verified as follows: given n disks, the largest disk must be moved at some point. To move the largest disk, the $n-1$ smaller disks must be moved out of the way first. Then, to complete the puzzle, the $n-1$ smaller disks must be moved back on top of the largest disk. Altogether, this process requires at least H_n moves.

Exercise

If you need help visualizing how this works, try it out online with an interactive version of the puzzle, e.g., see https://www.mathsisfun.com/games/towerofhanoi.html

The textbook has an illustration of the solution for 2 disks in Exercise 22.12, p. 147.

When you solve the puzzle with 3 disks, use the following strategy: (i) "pretend" that only the smallest 2 disks exist, and move them from peg 1 to peg 2; (ii) move the largest disk from peg 1 to peg 3; and (iii) "pretend" again that only the smallest 2 disks exist, and move them from peg 2 to peg 3, where you already placed the largest disk. See if you can reproduce the same strategy with 4 disks.

2.1.1 Substitution Method

The simplest method of solving recurrence relations, the **substitution method** (also called the "guess and check" method) exploits the fact that recurrence relations are recursively defined and, roughly speaking, we could find a solution to the recurrence relation by induction: take the initial terms as the base case, and take the recursive term to be the inductive case.

With the substitution method, we guess a solution to the recurrence relation and verify it's correctness by induction. Though this method is simple, it is not the most straightforward and intuitive method; there is no general heuristic to help in making a right guess. Making a wrong guess is possible, and a wrong guess means we have to start from scratch. However, with practice, the substitution method can become a quick way to check a potential solution without having to put in as much work as other methods require.

Example 20. By Lemma 19, we know that $H_n = 2H_{n-1} + 1$ is the recurrence for the Towers of Hanoi problem, and $H_1 = 1$. Now the question is: what is a closed form for H_n?

Let's make a guess... looking at the sequence H_n, it appears that the nth term is equal to $2^n - 1$. Is our guess correct? Check using a proof by induction. Let $S(n)$ be the statement $H_n = 2^n - 1$.

Base case: When $n = 1$, we have $2^1 - 1 = 1$. Since $H_1 = 1$, $S(1)$ is true.

Inductive hypothesis: Assume that $S(k)$ is true for some $k \in \mathbb{N}$ where $k \geq 1$. That is, assume that $H_k = 2^k - 1$.

Inductive case: We now show that $S(k+1)$ is true. By the inductive hypothesis, we have $H_k = 2^k - 1$. By our recurrence relation, we have

$$\begin{aligned} H_{k+1} &= 2H_k + 1 \\ &= 2(2^k - 1) + 1 \\ &= 2^{k+1} - 2 + 1 \\ &= 2^{k+1} - 1. \end{aligned}$$

Therefore, $S(k+1)$ is true. By the principle of mathematical induction, $S(n)$ is true for all $n \in \mathbb{N}$.

Note that, while the substitution method is good for proving easy solutions to recurrence relations, it can be a struggle to prove even a moderately-difficult solution using substitution.

2.1.2 Iteration Method

As opposed to the substitution method, which uses a proof by induction to find the closed form solution for a recurrence relation, the **iteration method** uses the recurrence relation itself to find its corresponding closed form. This method works by iteratively replacing occurrences of smaller terms in the recurrence relation with the corresponding equation for that term, then simplifying the expression. Once the initial terms are reached, the entire expression simplifies to the closed-form equation.

Example 21. Consider again the recurrence relation for the Towers of Hanoi problem: $H_n = 2H_{n-1} + 1$ and $H_1 = 1$. What is a closed form for H_n?

Using the iteration method, we proceed as follows:

$$\begin{aligned}
H_n &= 2H_{n-1} + 1 = 2(2H_{n-2} + 1) + 1 \\
&= 2^2 H_{n-2} + 2 + 1 = 2^2(2H_{n-3} + 1) + 2 + 1 \\
&= 2^3 H_{n-3} + 2^2 + 2 + 1 = 2^3(2H_{n-4} + 1) + 2^2 + 2 + 1 \\
&= 2^4 H_{n-4} + 2^3 + 2^2 + 2 + 1 \\
&\vdots \\
&= 2^{n-2} H_2 + 2^{n-3} + \cdots + 2 + 1 = 2^{n-2}(2H_1 + 1) + 2^{n-3} + \cdots + 2 + 1 \\
&= 2^{n-1} H_1 + 2^{n-2} + \cdots + 2 + 1 \\
&= 2^{n-1} + 2^{n-2} + \cdots + 2 + 1 \\
&= 2^n - 1.
\end{aligned}$$

The second-last line of the previous derivation is the sum of a geometric series: $\sum_{i=0}^{n-1} 2^i = \frac{2^{(n-1)+1}-1}{2-1} = 2^n - 1$.

2.1.3 First-Order Recurrence Relations

First-order recurrence relations are some of the easiest recurrence relations to deal with. Remember that we say a recurrence relation is “first-order” or “degree 1” if it produces new terms from only the previous term. In mathematical terms, a first-order recurrence relation is of the form

$$a_n = ca_{n-1} + x,$$

where the coefficient c and the additive term x are constants.

We can use the iteration method to obtain a general closed form for first-order recurrence relations. Observe that

$$\begin{aligned}
a_n &= ca_{n-1} + x \\
&= c(ca_{n-2} + x) + x \\
&= c^2(ca_{n-3} + x) + cx + x \\
&\vdots \\
&= c^{n-1}(ca_0 + x) + c^{n-2}x + c^{n-3}x + \cdots + cx + x \\
&= c^n a_0 + c^{n-1}x + c^{n-2}x + c^{n-3}x + \cdots + cx + x \\
&= c^n a_0 + (c^{n-1} + c^{n-2} + \cdots + c + 1)x.
\end{aligned}$$

Just like we saw in Example 21, the last line of the previous derivation includes a sum of a geometric series: $\sum_{i=0}^{n-1} c^i = \frac{c^n-1}{c-1}$. Altogether, we have

$$a_n = c^n a_0 + \left(\frac{c^n - 1}{c-1}\right) x,$$

and, by collecting like terms and rearranging, we get the general closed form which we state in the following theorem.

Theorem 22. *Let $a_n = ca_{n-1} + x$ be a recurrence relation where $c \neq 1$. Then the sequence $A_n = (a_1, a_2, \ldots, a_n, \ldots)$ is a solution of the recurrence relation if and only if*

$$a_n = \left(a_0 + \frac{x}{c-1}\right) c^n - \frac{x}{c-1}$$

for all $n \in \mathbb{N}$.

Proof. By the iteration method as done above. □

As Theorem 22 states, we cannot use this closed form if $c = 1$ because this would result in division by zero. Fortunately, another application of the iteration method to the similar recurrence relation $a_n = a_{n-1} + x$ gives us a result that works when $c = 1$.

Corollary 23. *Let $a_n = a_{n-1} + x$ be a recurrence relation. Then the sequence $A_n = (a_1, a_2, \ldots, a_n, \ldots)$ is a solution of the recurrence relation if and only if*

$$a_n = a_0 + nx$$

for all $n \in \mathbb{N}$.

Exercise

Show Corollary 23 using the iteration method.

2.1.4 Characteristic Root Method

So far, the methods we have seen for solving recurrence relations have been very general and very brute-force. With the substitution method, we resort to guessing and throwing induction at the problem. With the iteration method, we replace terms and simplify until something falls out of the expression that looks good. Although these methods work for many recurrence relations we need to solve, it would be nice to have a more refined method for solving recurrence relations.

Next we look at a method for solving a specific type of recurrence relation. In the general form, the **characteristic root method** is designed to solve linear homogeneous recurrence relations of degree k with constant coefficients. In other words, the characteristic root method solves recurrence relations of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where each of the coefficients $c_1, c_2, \ldots, c_k$ are real numbers and $c_k \neq 0$.

We've already seen a few examples of recurrence relations of this form; consider the Fibonacci sequence F_n or a_n from Example 14. Of course, not all recurrence relations are of this form; for instance, the recurrence relation for the pegs-and-disks problem, H_n, is not homogeneous because of its additive constant term. (This means we can't use H_n as our go-to example for the characteristic root method—but we already know how to solve the recurrence H_n.)

Where does the name "characteristic root method" come from? Characteristic roots are the values we use to solve the recurrence relation. From centuries of studying recurrence relations, mathematicians know that linear recurrence relations have exponential solutions; that is, solutions of the form $a_n = r^n$ for some constant r. We won't launch into any discussion about how mathematicians know this fact, since it's outside the scope of these notes. However, we observe that r^n is a solution of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$ if and only if

$$r^n = c_1 r^{n-1} + c_2 r^{n-2} + \cdots + c_k r^{n-k},$$

where we simply substitute all occurrences of a_i in the recurrence relation with r^i for $(n-k) \leq i \leq n$. If we divide both sides of this expression by r^{n-k} to get rid of the highest-order term on the right-hand side, then move all of the terms to one side, we end up with the equation

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_{k-1} r - c_k = 0. \tag{1}$$

We call such an expression the **characteristic equation** of the recurrence relation a_n, and we call the solutions of this equation the **characteristic roots** of a_n.

The roots of the equation (1) give a method for solving general k^{th} order recurrence relations. In the following we present the details only for 2nd order recurrence relations ($k = 2$) which is the case most commonly used. (Note that finding roots of 3rd or 4th order polynomials can be more complicated and the roots of 5th (or higher) order polynomials may not be possible to express in closed form.)

2.1.5 Second-Order Recurrence Relations with Two Characteristic Roots

The recurrence relations we deal with most frequently are second-order recurrence relations. The characteristic root method for recurrence relations of degree 2, in the case when the characteristic equation has two distinct roots, is based on the following result.

Proposition 24. *Let c_1 and c_2 be real numbers where $c_2 \neq 0$. Suppose that the recurrence relation*

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} \tag{2}$$

has a corresponding characteristic equation

$$r^2 - c_1 r - c_2 = 0$$

with two distinct roots r_1 and r_2. Then every solution of the recurrence (2) is of the form

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n,$$

$n \in \mathbb{N}$, where α_1 and α_2 are constants.

Proof. Omitted □

The constants α_1 and α_2 are typically determined by looking at values of a_n with small n.

Let's consider an example of the method in action with our favourite second-order recurrence relation defining the Fibonacci sequence F_n.

Example 25. Recall that $F_n = F_{n-1} + F_{n-2}$, where $F_1 = F_2 = 1$. What is a closed form for F_n?

From the statement of the recurrence relation for F_n, we see that $c_1 = 1$ and $c_2 = 1$, so the characteristic equation for F_n is

$$r^2 - r - 1 = 0.$$

The two distinct roots of this equation are $r_1 = (1+\sqrt{5})/2$ and $r_2 = (1-\sqrt{5})/2$. Therefore, the recurrence relation for F_n has a solution of the form

$$a_n = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^n$$

for all $n \in \mathbb{N}$, where α_1 and α_2 are constant.

To find the values of α_1 and α_2, we can use the initial terms of F_n. We have that

$$F_1 = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^1 + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^1 = 1 \text{ and}$$
$$F_2 = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^2 + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^2 = 1,$$

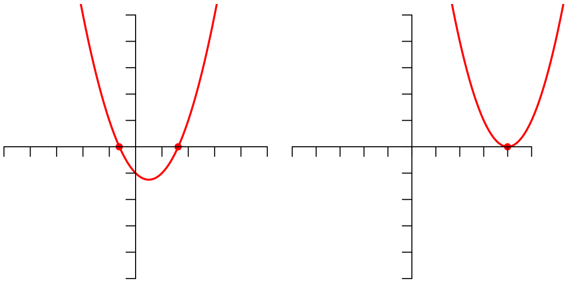
and solving these two expressions gives the values $\alpha_1 = 1/\sqrt{5}$ and $\alpha_2 = -1/\sqrt{5}$.

Therefore, the closed form for F_n is

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^n .$$

2.1.6 Second-Order Recurrence Relations with One Characteristic Root

Proposition 24 assumes that the characteristic equation has two distinct roots. However, we don't have a guarantee that a quadratic equation will always have two distinct roots. We may instead have two non-distinct roots, say, when the curve corresponding to the characteristic equation intersects the x-axis at exactly one point. Consider, for example, the following plots:



The plot on the left corresponds to the equation $r^2 - r - 1$, which we saw in Example 25. The plot on the right corresponds to an equation that intersects the x-axis only once; namely, the equation $r^2 - 8r + 16$. In this case, we are still able to use the characteristic root method, but we must make one small modification to its formulation. The proof of the following proposition is again omitted.

Proposition 26. *Let c_1 and c_2 be real numbers where $c_2 \neq 0$. Suppose that the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ has a corresponding characteristic equation*

$$r^2 - c_1 r - c_2 = 0$$

with exactly one root r_1. Then the recurrense has a solution of the form

$$a_n = \alpha_1 \, r_1^n + \alpha_2 \, n \, r_1^n$$

for $n \in \mathbb{N}$, where α_1 and α_2 are constants.

To make the characteristic root method work for characteristic equations with one root, we multiply the second term (that is, the term including α_2) by a factor of n.

Example 27. Consider the recurrence relation $g_n = 8g_{n-1} - 16g_{n-2}$ with initial terms $g_1 = 1$ and $g_2 = 6$. What is a closed form for g_n?

From the statement of the recurrence relation for g_n, we see that $c_1 = 8$ and $c_2 = -16$, so the characteristic equation for g_n is

$$r^2 - 8r + 16 = 0.$$

The only root of this equation is $r_1 = 4$. Therefore, the recurrence relation for g_n has a solution of the form

$$g_n = \alpha_1\, 4^n + \alpha_2\, n\, 4^n$$

for all $n \in \mathbb{N}$, where α_1 and α_2 are constants.

To find the values of α_1 and α_2, we can use the initial terms of g_n. We have that

$$\begin{aligned} g_1 &= \alpha_1\, 4^1 + \alpha_2\,(1)\,(4^1) = 4\,\alpha_1 + 4\,\alpha_2 = 1, \text{ and} \\ g_2 &= \alpha_1\, 4^2 + \alpha_2\,(2)\,(4^2) = 16\,\alpha_1 + 32\,\alpha_2 = 6, \end{aligned}$$

and solving these two equations gives the values $\alpha_1 = 1/8$ and $\alpha_2 = 1/8$.

Therefore, the closed form for g_n is

$$g_n = \frac{1}{8}\, 4^n + \frac{1}{8}\, n\, 4^n.$$

Exercise

For Example 27, to show that $g_n = \frac{1}{8}\, 4^n + \frac{1}{8}\, n\, 4^n$ is indeed the solution to the recurrence relation $g_n = 8g_{n-1} - 16g_{n-2}$, substitute the solutions $g_{n-1} = \frac{1}{8}\, 4^{n-1} + \frac{1}{8}\, n\, 4^{n-1}$ and $g_{n-2} = \frac{1}{8}\, 4^{n-2} + \frac{1}{8}\, n\, 4^{n-2}$ back into the recurrence relation. After simplifying the resulting expression, you should end up back with the original equation for the recurrence relation g_n.

Exercise

Solve the recurrence relation $a_n = 2a_{n-1} + 15a_{n-2}, a_0 = 4, a_1 = 0$. Verify your solution using the method described in the exercise above.