Introduction to Discrete Mathematics

Alexander Knop

January 17, 2019

Preface

If you are reading this book, you probably have never studied proofs before. So let me give you some advice: mathematical books are very different from fiction, and even books in other sciences. Quite often you may see that some steps are missing, and some steps are not really explained and just claimed as obvious. The main reason behind this is to make the ideas of the proof more visible and to allow grasping the essence of proofs quickly.

Since the steps are skipped, you cannot just read the book and believe that you studied the topic; the best way to actually study the topic is to try to prove every statement before you read the actual proof in the book. In addition to this, I recommend trying to solve all the exercises in the book (you may find exercises in the middle and at the end of every chapter).

Additionally, many topics in this book have a corresponding five-minute video explaining the material of the chapter, it is useful to watch them before you go into the topic.

Organization

Part 1 covers the basics of mathematics and provide the language we use in the next parts. We start from the explanation of what a mathematical proof is (in Chapter 1). Chapter 2 shows how to prove theorems indirectly using proof by contradiction. Chapter 3 explains the most powerful method in our disposal, proof by induction. Finally, Chapters 4-7 define several important objects such as sets, functions, and relations.

Alexander Knop
San Diego, California, USA

Contents

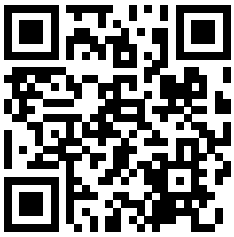
Part I

Introduction to Mathematical Reasoning

Chapter 1

Proofs

1.1 Direct Proofs



youtu.be/eJD0gGqveIE
What is a Mathematical Proof

We start the discussion of the proofs in mathematics from an example of a proof in "everyday" life. Assume that we know that the following statements are true.

1. If a salmon has fins and scales it is kosher,
2. if a salmon has scales it has fins,
3. any salmon has scales.

Using these facts we may conclude that any salmon is kosher; indeed, any salmon has scales by the third statement, hence, by the second statement any salmon has fins, finally, by the first statement any salmon is kosher since it has fins and scales.

One may notice that this explanation is a sequence of conclusions such that each of them is true because the previous one is true. Mathematical proof is also a sequence of statements such that every statement is true if the previous statement is true. If P and Q are some statements and Q is always true when P is true, then we say that P implies Q. We denote the statement that P implies Q by $P \implies Q$.

In order to define the implication formally let us consider the following table.

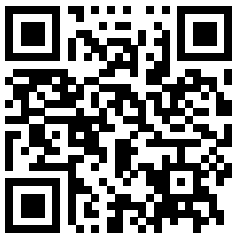
P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Let P and Q be some statements. Then this table says that if P and Q are both false, then $P \implies Q$ is true etc.

Exercise 1.1. *Let n be an integer.*

1. *Is it always true that "n^2 is positive" implies "n is not equal to 0"?*
2. *Is it always true that "$n^2 - n - 2$ is equal to 0" implies "n is equal to 2"?*

In the example we gave at the beginning of the section we used some *known* facts. But what does it mean to know something? In math we typically say that we know a statement if we can prove it. But in order to prove this statement we need to know something again, which is a problem! In order to solve it, mathematicians introduced the notion of an *axiom*. An axiom is a statement that is believed to be true and when we prove a statement we prove it under the assumption that these axioms are true[1].



youtu.be/nBjJi6aTk2M
What We Know and How to Find a Proof

For example, we may consider axioms of inequalities for real numbers.

1. Let $a, b \in \mathbb{R}$. Only one of the following is true:
   - $a < b$,
   - $b < a$, or
   - $a = b$.
2. Let $a, b, c \in \mathbb{R}$. Then $a < b$ iff $a + c < b + c$ (iff is an abbreviation for "if and only if").
3. Let $a, b, c \in \mathbb{R}$. Then $a < b$ iff $ac < bc$ provided that $c > 0$ and $a < b$ iff $ac > bc$ if $c < 0$.
4. Let $a, b, c \in \mathbb{R}$. If $a < b$ and $b < c$, then $a < c$.

Let us now try to prove something using these axioms, we prove that if $a > 0$, then $a^2 > 0$. Note that $a > 0$, hence, by the third axiom $a^2 > 0$.

Similarly, we may prove that if $a < 0$, then $a^2 > 0$. And combining these two statements together we may prove that if $a \neq 0$, then $a^2 > 0$.

Such a way of constructing proof is called direct proofs.

Exercise 1.2. *Axiomatic system for a four-point geometry.*
Undefined terms: point, line, is on.
Axioms:

- *For every pair of distinct points x and y, there is a unique line ℓ such that x is on l and y is on l.*
- *Given a line ℓ and a point x that is not on ℓ, there is a unique line m such that x is on m and no point on ℓ is also on m.*

[1] Note that in different parts of math axioms may be different

- *There are exactly four points.*
- *It is impossible for three points to be on the same line.*

Prove that there are at least two distinct lines.

Let n and m be some integers. Using direct proofs we may prove the following two statements.

- if n is even, then nm is also even[2],
- if n is even and m is even, then $n+m$ is also even.

We start from proving the first statement. There is an integer k such that $n = 2k$ since n is even. As a result, $nm = 2(nk)$ so nm is even.

Now we prove the second statement. Since n and m are even there are k and ℓ such that $n = 2k$ and $m = 2\ell$. Hence, $n + m = 2(k + \ell)$ so $n + m$ is even.

1.2 Constructing Proofs Backwards

However, sometimes it is not easy to find the proof. In this case one of the possible methods to deal with this problem is to try to prove starting from the end.

For example, we may consider the statement $(a+b)^2 = a^2+2ba+b^2$. Imagine, for a second, that you have not learned about axioms. In this case you would write something like this:

$$(a+b)^2 = (a+b)\cdot(a+b) = a(a+b)+b(a+b) = a^2+ab+ba+b^2 = a^2+2ba+b^2.$$

Let us try to prove it completely formally using the following axioms.

1. Let a, b, and c be reals. If $a = b$ and $b = c$, then $a = c$.
2. Let a, b, and c be reals. If $a = b$, then $a + c = b + c$ and $c + a = c + b$.
3. Let a, b, and c be reals. Then $a(b + c) = ab + ac$.
4. Let a and b be reals. Then $ab = ba$.
5. Let a and b be reals. Then $a + b = b + a$.
6. Let a be a real number. Then $a^2 = a \cdot a$ and $a \cdot a = a^2$.
7. Let a be a real number. Then $a + a = 2a$.

[2]A number n is even if there is an integer k such that $n = 2k$.

So the formal proof of the statement $(a+b)^2 = a^2 + 2ab + b^2$ is as follows. First note that $(a+b)^2 = (a+b)\cdot(a+b)$ (by axiom 6), hence, by axiom 1, it is enough to show that $(a+b)\cdot(a+b) = a^2 + 2ab + b^2$. By axiom 3, $(a+b)\cdot(a+b) = (a+b)\cdot a + (a+b)\cdot b$. Axiom 4 implies that $(a+b)\cdot a = a\cdot(a+b)$ and $(a+b)\cdot b = b\cdot(a+b)$ Hence, by axioms 1 and 2 applied twice

$$a\cdot(a+b) + b\cdot(a+b) = (a+b)\cdot a + b\cdot(a+b) = (a+b)\cdot a + (a+b)\cdot b.$$

As a result,

$$(a+b)\cdot(a+b) = (a+b)\cdot a + (a+b)\cdot b = a\cdot(a+b) + b\cdot(a+b) = a\cdot a + a\cdot b + b\cdot a + b\cdot b;$$

so by axiom 1, it is enough to show that $a\cdot a + a\cdot b + b\cdot a + b\cdot b = a^2 + 2ab + b^2$. Additionally, by axiom 6, $a\cdot a = a^2$ and $b\cdot b = b^2$. Hence, by axiom 2, it is enough to show that $a^2 + a\cdot b + b\cdot a + b^2 = a^2 + 2ab + b^2$. By axiom 4, $a\cdot b = b\cdot a$, hence, by axiom 2, $a\cdot b + b\cdot a = b\cdot a + b\cdot a$. Therefore by axiom 7, $a\cdot b + b\cdot a = 2b\cdot a$. Finally, by axiom 2, $a\cdot b + b\cdot a + a^2 + b^2 = 2b\cdot a + a^2 + b^2$ and by axiom 5, $a\cdot b + b\cdot a + a^2 + b^2 = a^2 + a\cdot b + b\cdot a + b^2$ and $2b\cdot a + a^2 + b^2 = a^2 + 2b\cdot a + b^2$. Which finishes the proof by axiom 1.

1.3 Analysis of Simple Algorithms

We can use this knowledge to analyze simple algorithms. For example, let us consider the following algorithm. Let us prove that it is correct i.e. it returns

Algorithm 1 The algorithm that finds the maximum element of a, b, c.

```
1: function MAX(a, b, c)
2:     r ← a
3:     if b > r then
4:         r ← b
5:     end if
6:     if c > r then
7:         r ← c
8:     end if
9:     return r
10: end function
```

the maximum of a, b, and c. We need to consider the following cases.

- If the maximum is equal to a. In this case, at line 2, we set $r = a$, at line 3 the inequality $b > r$ is false (since $a = r$ is the maximum) and at line 6 the inequality $c > r$ is also false (since $a = r$ is the maximum). Hence, we do not change the value of r after line 2 and the returned value is a.
- If the maximum is equal to b. We set $r = a$ at line 2. The inequality $b > r$ at line 3 is true (since b is the maximum) and we set r to be equal to b. So at line 6, the inequality $c > r$ is false (since $b = r$ is the maximum). Hence, the returned value is b.

- If the maximum is equal to c. We set $r = a$ at line 2. If the inequality $b > r$ is true at line 3 we set r to be equal to b. So at line 6 the inequality $c > r$ is true (since c is the maximum). Hence, we set r being equal to c and the returned value is c.

1.4 Proofs in Real-life Mathematics

In this chapter we explicitly used axioms to prove statements. However, it leads us to really long and hard to understand proofs (the last example in the previous section is a good example of this phenomenon). Because of this mathematicians tend to skip steps in the proofs when they believe that they are clear. This is the reason why it is arduous to read mathematical texts and it is very different from reading non-mathematical books. A problem that arises because of this tendency is that some mistakes may happen if we skip way too many steps. In the last two centuries there were several attempts to solve this issue, one approach to this we are going to discuss in the second part of this book.

End of The Chapter Exercises

1.3 Using the axioms of inequalities show that if a is a non-zero real number, then $a^2 > 0$.

1.4 Using the axioms of inequalities prove that for all real numbers a, b, and c,

$$bc + ac + ab \leq a^2 + b^2 + c^2.$$

1.5 Prove that for all integers a, b, and c, If a divides b and b divides c, then a divides c. Recall that an integer m divides an integer n if there is an integer k such that $mk = n$.

1.6 Show that square of an even integer is even.

1.7 Prove that 0 divides an integer a iff $a = 0$.

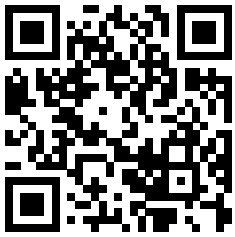
1.8 Using the axioms of inequalities, that if $a > 0$, b, and c are real numbers, then $b \geq c$ implies that $ab \geq ac$.

1.9 Using the axioms of inequalities, that if $a, b < 0$ are real numbers, then $a \leq b$ implies that $a^2 \geq b^2$.

Chapter 2

Proofs by Contradiction

2.1 Proving Negative Statements



youtu.be/bWP0VYx75DI

The direct method is not very convenient when we need to prove a negation of some statement.

For example, we may try to prove that $78n + 102m = 11$ does not have integer solutions. It is not clear how to prove it directly since we can not consider all possible n and m. Hence, we need another approach. Let us assume that such a solution n, m exists. Note that $78n+102m$ is even, but 11 is odd. In other words, an odd number is equal to an even number, it is impossible. Thus, the assumption was false.

Let us consider a more useful example, let us prove that if p^2 is even, then p is also even (p is an integer). Assume the opposite i.e. that p^2 is even but p is not. Let $p = 2b + 1$[1]. Note that $p^2 = (2b + 1)^2 = 2(2b^2 + 2b) + 1$. Hence, p^2 is odd which contradicts to the assumption that p^2 is even.

Using this idea we may prove much more complicated results e.g. one may show that $\sqrt{2}$ is irrational. For the sake of contradiction, let us assume that it is not true. In other words there are p and q such that $\sqrt{2} = \frac{p}{q}$ and $\frac{p}{q}$ is an irreducible fraction.

Note that $\sqrt{2}q = p$, so $2q^2 = p^2$. Which implies that p is even and 4 devises p^2. Therefore 4 devises $2q^2$ and q is also even. As a result, we get a contradiction with the assumption that $\frac{p}{q}$ is an irreducible fraction.

[1]Note that we use here the statement that an integer n is not even iff it is odd, which, formally speaking, should be proven.

Template for proving a statement by contradiction.

Assume, for the sake of contradiction, that *the statement* is false. Then *present some argument that leads to a contradiction.* Hence, the assumption is false and *the statement* is true.

Exercise 2.1. *Show that* $\sqrt{3}$ *is irrational.*

2.2 Proving Implications by Contradiction

This method works especially well when we need to prove an implication. Since the implication $A \implies B$ is false only when A is true but B is false. Hence, you need to derive a contradiction from the fact that A is true and B is false.

We have already seen such examples in the previous section, we proved that p^2 is even implies p is even for any integer p. Let us consider another example. Let a and b be reals such that $a > b$. We need to show that $(ac < bc) \implies c < 0$. So we may assume that $ac < bc$ but $c \geq 0$. By the multiplicativity of the inequalities we know that if $(a > b)$ and $c > 0$, then $ac > bc$ which contradicts to $ac < bc$.

A special case of such a proof is when we need to prove the implication $A \implies B$, assume that B is false and derive that A is false which contradicts to A (such proofs are called proofs by contraposition); note that the previous proof is the proof of this form.

2.3 Proof of "OR" Statements

Another important case is when we need to prove that at least one of two statements is true. For example, let us prove that $ab = 0$ iff $a = 0$ or $b = 0$. We start from the implication from the right to the left. Since if $a = 0$, then $ab = 0$ and the same is true for $b = 0$ this implication is obvious.

The second part of the proof is the proof by contradiction. Assume $ab = 0$, $a \neq 0$, and $b \neq 0$. Note that $b = \frac{ab}{a} = 0$, hence $b = 0$ which is a contradiction to the assumption.

End of The Chapter Exercises

2.2 Prove that if n^2 is odd, then n is odd.

2.3 In Euclidean (standard) geometry, prove: If two lines share a common perpendicular, then the lines are parallel.

2.4 Let us consider four-lines geometry, it is a theory with undefined terms: point, line, is on, and axioms:

1. there exist exactly four lines,

2. any two distinct lines have exactly one point on both of them, and
3. each point is on exactly two lines.

Show that every line has exactly three points on it.

2.5 Let us consider group theory, it is a theory with undefined terms: group-element and times (if a and b are group elements, we denote a times b by $a \cdot b$), and axioms:

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for every group-elements a, b, and c;
2. there is a unique group-element e such that $e \cdot a = a = a \cdot e$ for every group-element a (we say that such an element is the identity element);
3. for every group-element a there is a group-element b such that $a \cdot b = e$, where e is the identity element;
4. for every group-element a there is a group-element b such that $b \cdot a = e$, where e is the identity element.

Let e be the identity element. Show the following statements

- if $b_0 \cdot a = b_1 \cdot a = e$, then $b_0 = b_1$, for every group-elements a, b_0, and b_1.
- if $a \cdot b_0 = a \cdot b_1 = e$, then $b_0 = b_1$, for every group-elements a, b_0, and b_1.
- if $a \cdot b_0 = b_1 \cdot a = e$, then $b_0 = b_1$, for every group-elements a, b_0, and b_1.

2.6 Let us consider three-points geometry, it is a theory with undefined terms: point, line, is on, and axioms:

1. There exist exactly three points.
2. Two distinct points are on exactly one line.
3. Not all the three points are collinear i.e. they do not lay on the same line.
4. Two distinct lines are on at least one point i.e. there is at least one point such that it is on both lines.

Show that there are exactly three lines.

2.7 Show that there are irrational numbers a and b such that a^b is rational.

2.8 Show that there does not exist the largest integer.

Chapter 3

Proofs by Induction

3.1 Simple Induction

youtu.be/jOnZTWGpX_I

Let us consider a simple problem: what is bigger 2^n or n? In this chapter we are going to study the simplest way to prove that $2^n > n$ for all positive integers n. First let us check that it is true for small integers n.

n	1	2	3	4	5	6	7	8
2^n	2	4	8	16	32	64	128	256

We may also note that 2^n is growing faster than n, so we expect that if $2^n > n$ for small integers n, then it is true for all positive integers n

In order to prove this statement formally, we use the following principle.

Principle 3.1 (The Induction Principle)**.** *Let $P(n)$ be some statement about a positive integer n. Hence, $P(n)$ is true for every positive integer n iff*

base case: *$P(1)$ is true and*

induction step: *$P(k) \implies P(k+1)$ is true for all positive integers k.*

Let's prove now the statement using this principle. We define $P(n)$ be the statement that "$2^n > n$". $P(1)$ is true since $2^1 > 1$. Let us assume now that $2^n > n$. Note that $2^{n+1} = 2 \cdot 2^n > 2n \geq n + 1$. Hence, we proved the induction step.

Exercise 3.1. *Prove that $(1+x)^n \geq 1 + nx$ for all positive integers n and real numbers $x \geq -1$.*

3.2 Changing the Base Case

Let us consider functions n^2 and 2^n.

n	1	2	3	4	5	6	7	8
n^2	1	4	9	16	25	36	49	64
2^n	2	4	8	16	32	64	128	256

Note that 2^n is greater than n^2 starting from 5. But without some trick we can not prove this using induction since for $n = 3$ it is not true!

The trick is to use the statement $P(n)$ stating that $(n+4)^2 < 2^{n+4}$. The base case when $n = 1$ is true. Let us now prove the induction step. Assume that $P(k)$ is true i.e. $(k+4)^2 < 2^{k+4}$. Note that $2(k+4)^2 < 2^{k+1+4}$ but $(k+5)^2 = k^2 + 10k + 25 \leq 2k^2 + 8k + 32 = 2(k+4)^2$. Which implies that $2^{k+1+4} > (k+5)^2$. So $P(k+1)$ is also true.

In order to avoid this strange +4 we may change the base case and use the following argument.

Theorem 3.1. *Let $P(n)$ be some statement about an integer n. Hence, $P(n)$ is true for every integer $n > n_0$ iff*

base case: *$P(n_0 + 1)$ is true and*

induction step: *$P(k) \implies P(k+1)$ is true for all integers $k > n_0$.*

Using this generalized induction principle we may prove that $2^n \geq n^2$ for $n \geq 5$. The base case for $n = 4$ is true. The induction step is also true; indeed let $P(k)$ be true i.e. $(k+4)^2 < 2^{k+4}$. Hence, $2(k+4)^2 < 2^{k+1+4}$ but $(k+5)^2 = k^2 + 10k + 25 \leq 2k^2 + 8k + 32 = 2(k+4)^2$.

Let us now prove the theorem. Note that the proof is based on an idea similar to the trick with +4, we just used.

Proof of Theorem 3.1. $\Rightarrow$ If $P(n)$ is true for any $n > n_0$ it is also true for $n = n_0 + 1$ which implies the base case. Additionally, it true for $n = k+1$ so the induction step is also true.

$\Leftarrow$ In this direction the proof is a bit harder. Let us consider a statement $Q(n)$ saying that $P(n + n_0)$ is true. Note that by the base case for P, $Q(1)$ is true; by the induction step for P we know that $Q(n)$ implies $P(n+1)$. As a result, by the induction principle $Q(n)$ is true for all positive integers n. Which implies that $P(n)$ is true for all integers $n > n_0$.

□

3.3 Inductive Definitions

We may also define objects inductively. Let us consider the sum $1+2+\cdots+n$ a line of dots indicating "and so on" which indicates the definition by induction. In this case a more precise notation is $\sum_{i=1}^{n} i$.

Definition 3.1. *Let $a(1), \ldots, a(n), \ldots$ be a sequence of integers. Then $\sum_{i=1}^{n} a(i)$ is defined inductively by the following statements:*

- $\sum_{i=1}^{1} a(i) = a(1)$, *and*
- $\sum_{i=1}^{k+1} a(i) = \sum_{i=1}^{k} a(i) + a(k+1)$.

Let us prove that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Note that by definition $\sum_{i=1}^{1} i = 1$ and $\frac{1(1+1)}{2} = 1$; hence, the base case holds. Assume that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Note that $\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1)$ and by the induction hypothesis $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Hence, $\sum_{i=1}^{n+1} i = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}$.

Exercise 3.2. *Prove that $\sum_{i=1}^{n} 2^i = 2^{n+1} - 1$.*

3.4 Analysis of Algorithms with Cycles

Induction is very useful for analasing algorithms using cycles. Let us extend the example we considered in Section 1.3.

Let us consider the following algorithm. We prove that it is working correctly.

Algorithm 2 The algorithm that finds the maximum element of $a_1, \ldots, a_n$.

```
1: function MAX(a_1, ..., a_n)
2:     r ← a_1
3:     for i from 2 to n do
4:         if a_i > r then
5:             r ← a_i
6:         end if
7:     end for
8:     return r
9: end function
```

First, we need to define $r_1, \ldots, r_n$ the value of r during the execution of the algorithm. It is easy to see that $r_1 = a_1$ and $r_{i+1} = \begin{cases} r_i & \text{if } r_i > a_{i+1} \\ a_{i+1} & \text{otherwise} \end{cases}$. Secondly, we prove by induction that r_i is the maximum of $a_1, \ldots, a_i$. It is clear that the base case for $i = 1$ is true. Let us prove the induction step from k to $k+1$. By the induction hypothesis, r_k is the maximum of $a_1, \ldots, a_k$. We may consider two following cases.

- If $r_k > a_{k+1}$, then $r_{k+1} = r_k$ is the maximum of $a_1, \ldots, a_{k+1}$ since r_k is the maximum of $a_1, \ldots, a_k$.
- Otherwise, a_{k+1} is greater than $a_1, \ldots, a_k$, hence, $r_{k+1} = a_{k+1}$.

Exercise 3.3. *Show that line 6 in the following sorting algorithm executes $\frac{n(n+1)}{2}$ times.*

Algorithm 3 The algorithm is selection sort, it sorts $a_1, \ldots, a_n$.

```
1: function SelectionSort(a_1, ..., a_n)
2:     for i from 1 to n do
3:         r ← a_i
4:         ℓ ← i
5:         for j from i to n do
6:             if a_j > r then
7:                 r ← a_j
8:                 ℓ ← j
9:             end if
10:        end for
11:        Swap a_i and a_ℓ.
12:    end for
13: end function
```

3.5 Strong Induction

Sometimes $P(k)$ is not enough to prove $P(k+1)$ and we need all the statements $P(1), \ldots, P(k)$. In this case we may use the following induction principle.

Theorem 3.2 (The Strong Induction Principle)**.** *Let $P(n)$ be some statement about positive integer n. Hence, $P(n)$ is true for every integer $n > n_0$ iff*

base case: *$P(n_0 + 1)$ is true and*

induction step: *If $P(n_0 + 1), \ldots, P(n_0 + k)$ are true, then $P(n_0 + k + 1)$ is also true for all positive integers k.*

Before we prove this theorem let us prove some properties of Fibonacci numbers using this theorem. The Fibonacci numbers are defined as follows: $f_0 = 0$, $f_1 = 1$, and $f_k = f_{k-1} + f_{k-2}$ for $k \geq 3$.

Theorem 3.3 (The Binet formula)**.** *The Fibonacci numbers are given by the following formula*

$$f_n = \frac{\alpha^n - \beta^n}{\sqrt{5}},$$

where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$.

Proof. We use the strong induction principle to prove this statement with $n_0 = -1$. Let us first prove the base case, $\frac{(\alpha^0 - \beta^0)}{\sqrt{5}} = 0 = f_0$. We also need to prove the induction step.

- If $k = 1$, then $\frac{(\alpha^1 - \beta^1)}{\sqrt{5}} = 1 = f_1$.
- Otherwise, by the induction hypothesis, $f_k = \frac{\alpha^k - \beta^k}{\sqrt{5}}$ and $f_{k-1} = \frac{\alpha^{k-1} - \beta^{k-1}}{\sqrt{5}}$. By the definition of the Fibonacci numbers $f_{k+1} = f_k + f_{k-1}$. Hence,

$$f_{k+1} = \frac{\alpha^k - \beta^k}{\sqrt{5}} + \frac{\alpha^{k-1} - \beta^{k-1}}{\sqrt{5}}.$$

Note that it is enough to show that

$$\frac{\alpha^{k+1} - \beta^{k+1}}{\sqrt{5}} = \frac{\alpha^k - \beta^k}{\sqrt{5}} + \frac{\alpha^{k-1} - \beta^{k-1}}{\sqrt{5}}. \tag{3.1}$$

Note that it is the same as

$$\frac{\alpha^{k+1} - \alpha^k - \alpha^{k-1}}{\sqrt{5}} = \frac{\beta^{k+1} - \beta^k - \beta^{k-1}}{\sqrt{5}}.$$

Additionally, note that α and β are roots of the equation $x^2 - x - 1 = 0$. Hence, $\alpha^{k+1} - \alpha^k - \alpha^{k-1} = \alpha^{k-1}(\alpha^2 - \alpha - 1) = 0$ and $\beta^{k+1} - \beta^k - \beta^{k-1} = \beta^{k-1}(\beta^2 - \beta - 1) = 0$. Which implies that equality (3.1).

□

Now we are ready to prove the strong induction principle.

Proof of Theorem 3.2. It is easy to see that if $P(n)$ is true for all $n > n_0$, then the base case and the induction steps are true. Let us prove that if the base case and the induction step are true, then $P(n)$ is true for all $n > n_0$.

Let $Q(k)$ be the statement that $P(n_0 + 1)$, ..., $P(n_0 + k)$ are true. Note that $Q(1)$ is true by the base case for P. Additionally, note that if $Q(k)$ is true, then $Q(k+1)$ is also true, by the induction step for P. Hence, by the induction principle, $Q(k)$ is true for all positive integers k. Which implies that $P(n_0 + k)$ is true for all positive integers k. □

3.6 Recursive Definitions

Sometimes you wish to define objects using objects of the same form like in the case of inductive defenitions but you do not know how to enumerate them using an integer parameter.

One example of such a situation is the definition of an arithmetic formula.

base case: x_i is an arithmetic formula on the variables x_1, ..., x_n for all i.

recursion step: If P and Q are arithmetic formulas on the variables x_1, ..., x_n, then $(P + Q)$ and $P \cdot Q$ are arithmetic formulas on the variables x_1, ..., x_n.

Note that this definition implicitly state that any other expressions are not arithmetic formulas.

We can define recursively the value of such a formula. Let v_1, ..., v_n be some integers.

base case: $x_i\big|_{x_1=v_1,\ldots,x_n=v_n} = v_i$; in other words, the value of the arythmetic formula x_i is equal to v_1 when $x_1 = v_1$, ..., $x_n = v_n$.

recursion step: If P and Q are arythmetic formulas on the variables x_1, ..., x_n, then

$$(P+Q)\big|_{x_1=v_1,\ldots,x_n=v_n} = P\big|_{x_1=v_1,\ldots,x_n=v_n} + Q\big|_{x_1=v_1,\ldots,x_n=v_n}$$

and

$$(P\cdot Q)\big|_{x_1=v_1,\ldots,x_n=v_n} = P\big|_{x_1=v_1,\ldots,x_n=v_n} \cdot Q\big|_{x_1=v_1,\ldots,x_n=v_n}.$$

For example, $((x_1+x_2)\cdot x_3)$ is clearly an arithmetic formula on the variables x_1, ..., x_n. One may expect the value of this formula with $x_1=1$, $x_2=0$, and $x_3=-1$ be equal to -1, let us check:

- Note that
$$\begin{aligned} x_1\big|_{x_1=1,x_2=0,x_3=-1} &= 1, \\ x_2\big|_{x_1=1,x_2=0,x_3=-1} &= 0, \text{ and} \\ x_3\big|_{x_1=1,x_2=0,x_3=-1} &= -1. \end{aligned}$$
- Hence,
$$(x_1+x_2)\big|_{x_1=1,x_2=0,x_3=-1} = 1+0 = 1.$$
- Finally,
$$((x_1+x_2)\cdot x_3)\big|_{x_1=1,x_2=0,x_3=-1} = 1\cdot -1 = -1.$$

3.7 Analysis of Recursive Algorithms

To illustrate power of recursive definitions and strong induction, let us analyze Algorithm 4. We prove that number of comparisons of this algorithm is bounded by $6+2\log_2(n)$. First step of the proof is to denote the worst number of comparisons when we run the algorithm on the list of length n by $C(n)$. It is easy to see that $C(n)=n$ for $n\leq 5$. Additionally, $C(n)\leq 1+\max(C(\lfloor\frac{n}{2}\rfloor), C(n-\lfloor\frac{n}{2}\rfloor))$ for $n>5$. As we mentioned we prove that $C(n)\leq 6+2\log_2(n)$, we prove it by induction. The base case is clear; let us now prove the induction step. By the induction hypothesis,

$$C(\left\lfloor\frac{n}{2}\right\rfloor) \leq 6+2\log_2(\left\lfloor\frac{n}{2}\right\rfloor)$$

and

$$C(n-\left\lfloor\frac{n}{2}\right\rfloor) \leq 6+2\log_2(n-\left\lfloor\frac{n}{2}\right\rfloor).$$

Since $\lfloor\frac{n}{2}\rfloor \leq \frac{n}{2}$ and $n-\lfloor\frac{n}{2}\rfloor \leq \frac{n}{2}+1$, $C(n)\leq 1+2\log_2(\frac{n}{2}+1)$. However,

$$1+6+2\log_2\left(\frac{n}{2}+1\right) \leq 6+2\log_2\left(\frac{n}{\sqrt{2}}+\sqrt{2}\right) \leq 6+2\log_2(n)$$

for $n\geq 5$. As a result, we proved the induction step.

Algorithm 4 The binary search algorithm that finds an element e in the sorted list $a_1, \ldots, a_n$.

```
1: function BinarySearch(e, a_1, ..., a_n)
2:     if n ≤ 5 then
3:         for i from 1 to n do
4:             if a_i = e then
5:                 return i
6:             end if
7:         end for
8:     else
9:         ℓ ← ⌊n/2⌋
10:        if a_ℓ ≤ e then
11:            BinarySearch(e, a_1, ..., a_ℓ)
12:        else
13:            BinarySearch(e, a_{ℓ+1}, ..., a_n)
14:        end if
15:    end if
16: end function
```

End of The Chapter Exercises

3.4 Show that for any positive integer n, $n^2 + n$ is even.

3.5 Show that for any integer $n \geq 10$, $n^3 \leq 2^n$.

3.6 Show that for any positive integer n, $\sum_{i=0}^{n} x^i = \frac{1-x^{n+1}}{1-x}$.

3.7 Show that for any matrix $A \in \mathbb{R}^{m \times n}$ $(n > m)$ there is a nonzero vector $x \in \mathbb{R}^n$ such that $Ax = 0$.

3.8 Show that all the elements of $\{0,1\}^n$ (Binary strings) may be ordered such that every successive strings in this order are different only in one character. (For example, for $n = 2$ the order may be 00, 01, 11, 10.)

3.9 Let $a_0 = 2$, $a_1 = 5$, and $a_n = 5a_{n-1} - 6a_{n-2}$ for all integers $n \geq 2$. Show that $a_n = 3^n + 2^n$ for all integers $n \geq 0$.

3.10 Show that $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ for all integers $n \geq 1$.

3.11 Show that $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$.

3.12 Let $f_0 = 1$, $f_1 = 1$, and $f_{n+2} = f_{n+1} + f_n$ for all $n \in \mathbb{N}$. Show that $f_n \geq \left(\frac{3}{2}\right)^{n-2}$.

3.13 Show that $f_{n+m} = f_{n-1}f_m + f_n f_{m+1}$.

3.14 Show that two arythmetic formulas $(x_1 + x_2) \cdot x_3$ and $x_1 \cdot x_3 + x_2 \cdot x_3$ on the variables x_1, x_2, and x_3 have the same values.