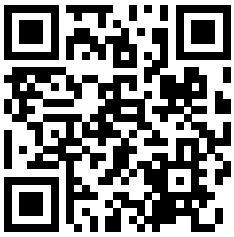
Chapter 1

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.

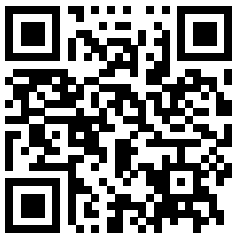
P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

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, show 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, show that if $a, b < 0$ are real numbers, then $a \leq b$ implies that $a^2 \geq b^2$.