Math 220 Fall 2021, Lecture 11: Deduction rules

0.1. Deduction rules (cont'd)

0.1.1. Proof by contradiction II

Proof by contradiction II: Let P be a proposition. Assume that you have proved a contradiction under the assumption of NOT P. Then, you can deduce that P.

> **Example 0.1.1.** Let a and b be two integers such that ab is even. We claim that a or b is even.
>
> We prove this as follows: Assume that NOT (a or b is even). In other words, assume that neither a nor b is even. Thus, by de Morgan's laws (specifically, the law that says (NOT (P OR Q)) $\Longleftrightarrow$ ((NOT P) AND (NOT Q))), both a and b are non-even. In other words, both a and b are odd. Hence, we can write a and b in the forms
>
> $$a = 2n + 1 \qquad \text{and} \qquad b = 2m + 1$$
>
> for some integers n and m. (This is a consequence of division with remainder, which we take for granted at this point; soon we will see it proved as well.) Now, multiplying the equalities $a = 2n + 1$ and $b = 2m + 1$, we obtain
>
> $$ab = (2n + 1)(2m + 1) = 4nm + 2n + 2m + 1 = 2(2nm + n + m) + 1.$$
>
> Hence, ab is an integer of the form $2k + 1$ for some $k \in \mathbb{Z}$ (namely, for $k = 2nm + n + m$). Since all such integers are odd (another consequence of division with remainder), we thus conclude that ab is odd. In other words, ab is not even. However, we know that ab is even. The previous two sentences result in a contradiction.
>
> Thus, we have proved a contradiction under the assumption that NOT (a or b is even). Therefore, by the "proof by contradiction II" rule, we conclude that a or b is even.

When making proofs like this in practice, you normally start them by saying "Assume the contrary". This simply says that you are assuming NOT P, where P is whatever claim you just made. (In our above example, P is "a or b is even".) Once you have obtained your contradiction, you then say "Thus, the assumption must have been wrong, so we conclude that P holds". This kind of proof is called "proof by contradiction" or "indirect proof".

Note that versions I and II of the "proof by contradiction" rule are more or less equivalent. Indeed, we know that NOT (NOT P) is equivalent to P. Thus, if you can deduce one of these, you can also deduce the other (by $\Longleftrightarrow$-elimination).

0.1.2. Disjunctive syllogism

Disjunctive syllogism: Let P and Q be two propositions. Assume that you have proved P OR Q and proved NOT P. Then you can deduce Q.

> **Example 0.1.2.** You know that 7 is even or odd. You know that 7 is not even. Hence, 7 is odd.

Actually, the "disjunctive syllogism" rule follows from Modus Ponens (since we know that $((P \text{ OR } Q) \text{ AND } (\text{NOT } P)) \Longrightarrow Q$). But we state it as a separate deduction rule, because mathematicians tend to just use it as a single move.

0.1.3. OR-elimination, aka Case distinction (aka Case analysis)

OR-elimination: Let P, Q and R be three propositions. Assume that you have proved $P \Longrightarrow R$ and proved $Q \Longrightarrow R$ and proved P OR Q. Then, you can deduce R.

The idea behind this is that if you can prove R when P holds, and you can prove R when Q holds, but you know that P OR Q holds, then you can deduce R. This kind of reasoning is called "proof by cases" or "case distinction" or "case analysis".

> **Example 0.1.3.** We claim that for any integer n, we have $n^2 \geq n$.
>
> We prove this as follows: Let n be an integer. Then, $n \geq 1$ OR $n < 1$.
>
> Now, let us show that $(n \geq 1) \Longrightarrow (n^2 \geq n)$.
>
> Indeed, assume that $n \geq 1$. Thus, $n \geq 1 \geq 0$ and $n - 1 \geq 0$. Recall that the product of two nonnegative integers is again nonnegative. Hence, from $n \geq 0$ and $n - 1 \geq 0$, we obtain $n(n-1) \geq 0$. This rewrites as $n^2 - n \geq 0$ (by expanding). In other words, $n^2 \geq n$.
>
> Thus we have showed that $(n \geq 1) \Longrightarrow (n^2 \geq n)$.
>
> Next, let us show that $(n < 1) \Longrightarrow (n^2 \geq n)$.
>
> Indeed, assume that $n < 1$. Then, $n \leq 0$ (since n is an integer). Hence, $n - 1 \leq -1 \leq 0$. Recall that the product of two nonpositive integers is nonnegative. Hence, from $n \leq 0$ and $n - 1 \leq 0$, we obtain $n(n-1) \geq 0$. This rewrites as $n^2 - n \geq 0$ (by expanding). In other words, $n^2 \geq n$.
>
> Thus we have showed that $(n < 1) \Longrightarrow (n^2 \geq n)$.
>
> Now, we have proved that $(n \geq 1) \Longrightarrow (n^2 \geq n)$ and proved that $(n < 1) \Longrightarrow (n^2 \geq n)$ and proved that $n \geq 1$ OR $n < 1$. Hence, by OR-elimination, we conclude that $n^2 \geq n$, qed.

Recall: The word "qed" means "The proof is complete now".

Here is how the above proof would be written in standard mathematical language:

"Let n be an integer. Then, $n \geq 1$ or $n < 1$. Thus, we must be in one of the following two cases:

Case 1: We have $n \geq 1$.

Case 2: We have $n < 1$.

Let us first consider Case 1. In this case, we have $n \geq 1$. Thus, $n \geq 1 \geq 0$ and $n - 1 \geq 0$. Recall that the product of two nonnegative integers is again nonnegative. Hence, from $n \geq 0$ and $n - 1 \geq 0$, we obtain $n(n-1) \geq 0$. This rewrites as $n^2 - n \geq 0$ (by expanding). In other words, $n^2 \geq n$. Thus, our claim is proved in Case 1.

Let us next consider Case 2. In this case, we have $n < 1$. Thus, $n \leq 0$ (since n is an integer). Hence, $n - 1 \leq -1 \leq 0$. Recall that the product of two nonpositive integers is nonnegative. Hence, from $n \leq 0$ and $n - 1 \leq 0$, we obtain $n(n-1) \geq 0$. This rewrites as $n^2 - n \geq 0$ (by expanding). In other words, $n^2 \geq n$. Thus, our claim is proved in Case 2.

We have now proved our claim in both cases 1 and 2. So the claim is proved in general."

More generally, we can distinguish between several cases at once:

k-**OR-elimination:** Let $P_1, P_2, \ldots, P_k$ and R be propositions. Assume that you have proved $P_1 \Longrightarrow R$ and proved $P_2 \Longrightarrow R$ and $\cdots$ and proved $P_k \Longrightarrow R$ and proved P_1 OR P_2 OR P_3 OR $\cdots$ OR P_k. Then, you can deduce R.

Proofs using this rule (which follows from the original OR-elimination rule by applying the latter several times) are again called "proofs by cases"; this time, there are k cases instead of two.

Here is a more complicated example of proof by cases:

Recall that for any real number z, the **absolute value** $|z|$ is defined to be

$$\begin{cases} z, & \text{if } z \geq 0; \\ -z, & \text{if } z < 0. \end{cases}$$

Theorem 0.1.4 (triangle inequality for reals)**.** For any real numbers x and y, we have $|x| + |y| \geq |x + y|$.

Proof. We have $x \geq 0$ or $x < 0$. Thus, we are in one of the following two cases:

Case 1: We have $x \geq 0$.

Case 2: We have $x < 0$.

Let us first consider Case 1. In this case, we have $x \geq 0$. Thus, $|x| = x$. We have $y \geq 0$ or $y < 0$. Thus, we are in one of the following two subcases (= cases, except nested inside an already existing case):

Subcase 1.1: We have $y \geq 0$.

Subcase 1.2: We have $y < 0$.

Let us first consider Subcase 1.1. In this subcase, we have $y \geq 0$. Thus, $|y| = y$. Now, from $x \geq 0$ and $y \geq 0$, we obtain $x + y \geq 0$, so that $|x + y| = x + y$. Now,

$$|x| + |y| = x + y = |x + y|.$$

Hence, our claim is proved in Subcase 1.1.

Let us next consider Subcase 1.2. In this subcase, we have $y < 0$. Thus, $|y| = -y$. Now, $x + y \geq 0$ or $x + y < 0$. Thus, we are in one of the following subsubcases:

Subsubcase 1.2.1: We have $x + y \geq 0$.

Subsubcase 1.2.2: We have $x + y < 0$.

Let us first consider Subsubcase 1.2.1. In this subsubcase, we have $x + y \geq 0$. Thus, $|x + y| = x + y$. Now,

$$|x| + |y| = x + \underbrace{(-y)}_{\geq 0 \geq y} \geq x + y = |x + y| .$$

Hence, our claim is proved in Subsubcase 1.2.1.

Let us next consider Subsubcase 1.2.2. In this subsubcase, we have $x + y < 0$. Thus, $|x + y| = -(x + y)$. Now,

$$|x| + |y| = x + (-y) = \underbrace{x}_{\geq 0 \geq -x} -y \geq -x - y = -(x + y) = |x + y| .$$

Hence, our claim is proved in Subsubcase 1.2.2.

Now, we have covered the entire Case 1.

Next, it remains to study Case 2. This will be a HW problem. □

Alternatively, we could have avoided subcases and subsubcases by restating the above proof as an analysis of six cases:

Case 1: We have $x \geq 0$ and $y \geq 0$.

Case 2: We have $x \geq 0$ and $y < 0$ and $x + y \geq 0$.

Case 3: We have $x \geq 0$ and $y < 0$ and $x + y < 0$.

Case 4: ...

Case 5: ...

Case 6: ...

0.2. Proof by counterexample

Proof by counterexample: Let S be a set. Let $P(x)$ be a predicate that depends on a variable x which is supposed to belong to S. Let $s \in S$.

Assume that you have proved that NOT $P(s)$. Then you can deduce that NOT $(\forall x \in S : P(x))$.

(For example, if you have proved that 3 is not even, then you can deduce that not all integers are even.)

In such a case, s is called a **counterexample** to $\forall x \in S : P(x)$.

Likewise, when you derive $\exists x \in S : P(x)$ from $P(s)$, the s is called an **example** (or **witness**) for $\exists x \in S : P(x)$.

Remark 0.2.1. A single counterexample is sufficient to disprove a $\forall$-statement, but not to disprove an $\exists$-statement.

A single example is sufficient to prove an $\exists$-statement, but not to prove a $\forall$-statement.

This all is nothing new – it's a consequence of proof by contradiction.

1. Mathematical induction

1.1. What is induction?

The above deduction rules constitute what is known as **first-order logic**. They allow us to prove properties of sets, such as $(A \triangle B) \triangle C = A \triangle (B \triangle C)$, and properties of logical propositions. In our above examples, we have used them to prove properties of numbers as well – however, we have not been fully honest, because we have used certain fundamental properties without proof. For example, how do we know that every integer n satisfies $n \geq 1$ or $n < 1$? How do we know that any odd (= non-even) integer can be written as $2k + 1$ for some integer k ? How do we know (recalling back our proof of the infinitude of primes) that any integer > 1 has a smallest divisor > 1 ?

You can imagine assuming these facts as axioms. However, if you try to prove deeper properties of numbers using the above deduction rules, you will need more and more axioms, as you will run into more and more situations like these. The problem is that we don't know what integers **are**.

So we need a new rule, for proving facts about integers in particular. Even better, we shall start with nonnegative integers. These are a good springboard, since all other kinds of numbers (integers, rationals, reals, and more) can be defined in terms of nonnegative integers.

We let $\mathbb{N}$ be the set of nonnegative integers.

As we recall, these nonnegative integers are $0, 1, 2, 3, 4, 5, \ldots$. If we take 0 and 1 for granted, all of them can be constructed by repeatedly adding 1 to 0. For instance,

$$7 = 0 + 1 + 1 + 1 + 1 + 1 + 1 + 1.$$

Thus, the essence of the nonnegative integers is that they form an "infinite ladder" (or chain or sequence), with each one having a well-defined successor and (except for 0) a well-defined predecessor. Each nonnegative integer can be reached from 0 by climbing this ladder.

It stands to reason that a proposition about nonnegative integers (i.e., a proposition of the form "$\forall n \in \mathbb{N} : P(n)$") should be provable in the following way: First you show that it holds for 0 (that is, you show that $P(0)$ is true), and then you show that if it holds for a nonnegative integer n, then it also holds for the next integer $n + 1$. Metaphorically, you show that it holds at the base of the ladder, and then you show that you can "carry it up" one step. Since all nonnegative integers are reachable, this then allows you to carry it to any rung of the ladder.

Here is the formal statement of this one last deduction rule:

> **Principle of Mathematical Induction** (or, short, **Principle of Induction):**
>
> Let $P(n)$ be a predicate that depends on a variable n, which is supposed to be a nonnegative integer.
>
> Assume that you have proved $P(0)$.

Assume further that you have proved

$$\forall n \in \mathbb{N} : \left(P\left(n\right) \Longrightarrow P\left(n+1\right)\right).$$

Then, you can deduce that

$$\forall n \in \mathbb{N} : P\left(n\right).$$

Next time, we will actually use this to prove some statements, some of them interesting(?).