EECS/MATH 1019
Section 1.7: Introduction to Proofs — continued
Section 1.8.2: Proof by Cases

January 19, 2023

Proofs

A proof is a logical argument that is written to convince the reader that a particular proposition is true.

Each step in a proof should have a clear reason for why it is true.

In this section, and in most of the rest of this course, we shall work with "informal" proofs that are somewhat less constrained than the "formal" logical arguments of Sections 1.1–1.6, where every single step needed justification by an explicit rule or formula chosen from a small list.
We can think of a formal logical proof as something that a machine could read and verify, while an informal proof is something for a human being to read and verify.

An informal proof should be logically complete and correct, and should be written so that the reader can comprehend the overall structure and the details of the logical argument unambiguously. Precision and clarity are essential.

In the last class, we proved the following.

Proposition 1.A. *Let n be an integer. Then n^2 is even if and only if n is even.*

Here another way to state the proposition:

Proposition 1.A. *For every integer n, (n^2 is even) $\leftrightarrow$ (n is even).*

Before we tried to find a proof, we needed to be clear what we mean by "even."

Definition: An integer m is *even* if there exists an integer k such that $m = 2k$. An integer m is *odd* if there exists an integer k such that $m = 2k + 1$.

Every integer is either even or odd.

Proposition 1.A. *For every integer n, (n^2 is even) $\leftrightarrow$ (n is even).*

We also recalled that $p \leftrightarrow q$ is equivalent to $(p \to q) \wedge (q \to p)$.
So Proposition 1.A is equivalent to the following:

Proposition 1.A. *Let n be an integer.*
(a) If n is even, then n^2 is even.
(b) If n^2 is even, then n is even.

To prove Proposition, we proved parts (a) and (b) separately.

Proof of (a): Assume n is even. Then $n = 2k$ for some integer k.
Then
$$n^2 \;=\; (2k)^2 \;=\; 2(2k^2)\,.$$
Since $n^2 = 2(2k^2)$ and $2k^2$ is an integer, it follows that n^2 is even.
This proves part (a).
(This kind of proof often is called a “direct proof.”)

Proposition 1.A. *Let n be an integer.*

(b) If n^2 is even, then n is even.

Instead of a direct proof of (b), we did the following.

Recall that the contrapositive of the statement $p \to q$ is the statement $\neg p \to \neg q$, and that these two statements are logically equivalent: that is, $(p \to q) \equiv (\neg q \to \neg p)$.

The contrapositive of (b) is

(b') If n is not even, then n^2 is not even.

Proof of (b'): Assume n is not even. Then n is odd. Therefore $n = 2k + 1$ for some integer k. Then

$$n^2 \ = \ (2k+1)^2 \ = \ 4k^2 + 4k + 1 \ = \ 2(2k^2 + 2k) \ + \ 1.$$

Since $n^2 = 2(2k^2 + 2k) + 1$ and $(2k^2 + 2k)$ is an integer, it follows that n^2 is odd. Hence n^2 is not even. This proves (b').

Since (b') is logically equivalent to (b), we have proved (b).

And this completes the proof of Proposition 1.A. Q.E.D.

(The proof of (b) is an example of an "indirect proof.")

Another useful method of indirect proof is called "Proof by contradiction." Here is the idea.
Suppose we want to prove that P is true. Suppose we can find a False statement C (a "contradiction") such that $(\neg P) \rightarrow C$ is true. Then $\neg P$ must be False, that is, P must be true.

Here is a famous example.

First, we introduce a defintion.
Definition: A real number x is *rational* if we can write $x = m/n$ for some integers m and n (with $n \neq 0$). A real number is *irrational* if it is not rational.

E.g. Some rational numbers are $\frac{-491}{1229}$, 0, and $3.22 = \frac{322}{100}$.

Theorem 1.B (= Example 11 in Sec 1.7). The square root of 2 is irrational.

This was first proved by the Pythagoreans in ancient Greece, about 2500 years ago.

Theorem 1.B. The square root of 2 is irrational.

Proof of Theorem 1.B: We shall give a proof by contradiction. Assume that $\sqrt{2}$ is a rational number r. Then $r^2 = 2$. We can write $r = \frac{m}{n}$ where m and n are integers with no common factor greater than 1. (In other words, express r in "lowest terms.") Then

$$2 = r^2 = \frac{m^2}{n^2}. \quad \text{Therefore} \quad 2n^2 = m^2.$$

Therefore m^2 is even. By Proposition 1.A, we infer that m is even. That is, $m = 2k$ for some integer k. Since $2n^2 = m^2$, we obtain

$$2n^2 = (2k)^2 = 4k^2. \quad \therefore \quad n^2 = 2k^2. \quad \text{Hence } n^2 \text{ is even.}$$

By Proposition 1.A (again), we infer that n is even. Since m and n are both even, they have 2 as a common factor. This contradicts the assertion that m and n have no common factors greater than 1. We conclude that $\sqrt{2}$ cannot be rational. Q.E.D.

What about the following proposition?

If s and t are integers, then $s + t\sqrt{2}$ is irrational.

It is False because there is a counterexample. E.g. Suppose $s = 5$ and $t = 0$. These are integers, but $s + t\sqrt{2} = 5 + 0\sqrt{2} = 5 = \frac{5}{1}$. which is NOT irrational.

Let's try to salvage this proposition by not allowing t to be 0.

Proposition 1.C: *If s and t are integers, and $t \neq 0$, then $s + t\sqrt{2}$ is irrational.*

Exercise: Prove Proposition 1.C using proof by contradiction. You may use the result of Theorem 1.B.

Prove the following:

Let a, b, and c be consecutive integers, with $a < b < c$ (e.g., 16, 17, 18; or, -90, -89, -88.) Prove that $a + 2b + c$ must be even.

(*First think how we can we express the information we are given about a, b, and c.*)

We know that $b = a + 1$ and $c = b + 1 = a + 2$. Then we have

$$a + 2b + c \ = \ a + 2(a + 1) + (a + 2) \ = \ 4a + 4 \ = \ 2(2a + 2).$$

(*Now draw the conclusion:*)
Since $a + 2b + c = 2(2a + 2)$ and $2a + 2$ is an integer, we conclude that $a + 2b + c$ is even. Q.E.D.

(*If we leave out the italicized comments, then we have a valid and well written proof.*)

Proof by cases (Section 1.8.2):

We saw one example of "Proof by cases" in the class of January 12, where we proved

$$W: \quad \text{If } \forall x\,[P(x) \leftrightarrow Q(x)], \text{ then } [\forall x\, P(x)] \leftrightarrow [\forall x\, Q(x)].$$

We considered two cases:
(a) $[\forall x\, P(x)]$ is true, or
(b) $\neg[\forall x\, P(x)]$ is true (i.e., $[\forall x\, P(x)]$ is false),
and showed that W is true in each case.

Idea: Let V be the statement $[\forall x\, P(x)]$.
We know $V \to W$ from part (a), and $\neg V \to W$ from part (b).
Then we can conclude that W is true.

<u>Exercise:</u> Verify this last assertion in two different ways:
(i) use the "Resolution" argument in Section 1.6;
(ii) Show that $(V \to W) \wedge (\neg V \to W) \equiv W$ using rules of Section 1.3.

Example 1.8.A: Prove that $n^2 - 3n + 6$ is even for every integer n.

One way to prove this is to consider two cases for an integer n:
(a) n is even or (b) n is odd.

Assume (a). Then $n = 2k$ for some integer k, and

$$n^2 - 3n + 6 \;=\; (2k)^2 - 3(2k) + 6 \;=\; 4k^2 - 6k + 6 \;=\; 2(2k^2 - 3k + 3).$$

Since $(2k^2 - 3k + 3)$ is an integer, we see that $n^2 - 3n + 6$ is even.

Now assume (b). Then $n = 2j + 1$ for some integer j, and

$$\begin{aligned} n^2 - 3n + 6 &= (2j+1)^2 - 3(2j+1) + 6 \\ &= (4j^2 + 4j + 1) - 6j - 3 + 6 \\ &= 4j^2 - 2j + 4 \quad = 2(2j^2 - j + 2). \end{aligned}$$

Since $(2j^2 - j + 2)$ is an integer, we see that $n^2 - 3n + 6$ is even.
Since $n^2 - 3n + 6$ is even in each case, we conclude that it is always even. Q.E.D.

Summary: For $W(n)$: "$n^2 - 3n + 6$ is even" and $V(n)$: "n is even," we proved $\forall n\,([V(n) \to W(n)] \wedge [\neg V(n) \to W(n)])$, which is equivalent to $\forall n\, W(n)$.

More generally, we can consider more than two cases. For example, if we know that one of the statements V_1 or V_2 or V_3 or V_4 or V_5 is true, and we know that $V_i \to W$ for each $i = 1, 2, 3, 4, 5$, then we can conclude that W is true.

Example 1.8.B: Let x and y be integers. Prove that if $x + y$ is odd then xy is even.

One way to prove this is to consider three cases for a given pair of integers x and y:
(a) both x and y are even;
(b) both x and y are odd;
(c) one is even and the other is odd.

In case (a), $x + y$ is not odd [fill in the details], so the statement "If $x + y$ is odd, then xy is even" is true ("vacuous proof").

Similarly, case (b) is (vacuously) true [fill in the details].

Example 1.8.B: Let x and y be integers. Prove that if $x + y$ is odd then xy is even.

Consider three cases for a given pair of integers x and y:
(a) both x and y are even;
(b) both x and y are odd;
(c) one is even and the other is odd.

- - - - - - - - - - - - - - - - -

Continuation:

In case (c), we can assume *without loss of generality* that x is even and y is odd. (That is, the argument would be essentially the same if we assumed that x is odd and y is even.)
Then ??????

Remark: When doing a proof by cases, you must make sure that the cases together cover all possibilities. If one possibility is missing, then it could be the case for which the desired result is not true.
(See Examples 8 and 9 in Section 1.8.)

Next class: Read the rest of Section 1.8. On first reading, focus on subsections up to and including 1.8.6.

Homework 1 is posted in Connect, due Sunday Jan 22 at 11:59 pm.

Homework 2 will be posted in a day or two, due Sunday Jan 29.