LECTURE 3

Methods of Proof, cont'd

Last time we discussed some of the basic techniques for proving propositions. We began with the notion of a **direct proof** and one of its implementations, the **forward-backward method**. Then we discussed an alternative to the direct proof, **proof by contradiction**.

I would like to begin today's lecture with another example of proof by contradiction.

EXAMPLE 3.1. Use the method of proof by contradiction to show that the equation

$$x^2 + 2mx + 2n = 0$$

has no odd roots if m and n are odd.

This proposition is equivalent to one of the form $P \Rightarrow Q$ if we take P to be the statement "m and n are odd integers", and Q to be the statement "there exists no odd integer x such that $x^2 + 2mx + 2n = 0$". Not-Q is then the statement that there exists an odd integer x such that $x^2 + 2mx + 2n = 0$.

To apply the method of proof by contradiction, we suppose P and not-Q are true and look for a contradiction with known facts.

So let x be an odd integer satisfying

$$x^2 + 2mx + 2n = 0$$

and suppose both m and n are odd. Then

$$x^2 = -2(mx + n) \quad .$$

The right hand side, being a multiple of 2, is clearly even. So x^2 is even. On the other hand, x is supposed to be odd. In your last homework assignment you proved (hopefully) that if x is odd, then x^2 is necessarily odd. We have thus arrived at a contradiction with a known fact. Since P and not-Q can not be simultaneously true, we have

$$\text{"}P \text{ is true"} \Rightarrow \text{"not-}Q \text{ is false"}$$

or

$$P \Rightarrow Q \quad .$$

$\square$

1. The Contrapositive Method

The **contrapositive method** is a variation of the proof by contradiction method in which one tries to work forward from the hypothesis "not-Q is true" to conclude that "not-P" is true. For if we can show that

$$\text{not-}Q \Rightarrow \text{not-}P$$

then we can conclude that

$$P \Rightarrow Q \quad .$$

The justification for conclusion runs as follows:

(i) $$\text{"}P \text{ is true"} \Rightarrow \text{"not-}P \text{ is false"}$$

(ii) "not-P is false" and "not-Q $\Rightarrow$ not-P is true" $\Rightarrow$ "not-Q is false"

(iii) "not-Q is false" $\Rightarrow$ "Q is true"

EXAMPLE 3.2. Let's use the contrapositive method to prove

PROPOSITION 3.3. *If n is an integer and n^2 is an odd integer, then n is odd.*

proof.

In this proposition the hypothesis P is "n is an integer and n^2 is an odd integer" and the conclusion Q we're trying to reach is "n is odd". So

$$\begin{aligned} \text{not-}Q &= n \text{ is not even} \\ \text{not-}P &= n \text{ is not an integer or } n^2 \text{ is not an odd integer} \end{aligned}$$

In figuring out not-P we used the rule that not-(A and B) = not-A or not-B. However, this makes our new conclusion more complicated then necessary.

Let's instead first rephrase the statement we're trying to prove as

Suppose n is an integer. Then n^2 is an odd integer implies n is odd

or diagramatically

$$n \in \mathbb{Z} \quad \Rightarrow \quad \left(n^2 \text{ is odd} \quad \Rightarrow \quad n \text{ is odd}\right)$$

But then the contrapositive of the propositional statement in parentheses is

$$n \text{ is not-odd} \quad \Rightarrow \quad n^2 \text{ is not-odd}$$

or

$$n \text{ is even} \quad \Rightarrow \quad n^2 \text{ is even}$$

Since the contrapositive is true (we've shown this in an earlier example), the original propositional statement is true.

Here is the entire proof. The statement

"If n is an integer and n^2 is an odd integer, then n is odd"

is equivalent to

$$\text{"}n \in \mathbb{Z} \quad \Rightarrow \quad \left(n^2 \text{ is odd} \quad \Rightarrow \quad n \text{ is odd}\right)\text{"}$$

which is equivalent to

$$\text{"}n \in \mathbb{Z} \quad \Rightarrow \quad \left(n \text{ is not-odd} \quad \Rightarrow \quad n^2 \text{ is not odd}\right)\text{"}$$

which is equivalent to

$$\text{"}n \in \mathbb{Z} \quad \Rightarrow \quad \left(n \text{ is even} \quad \Rightarrow \quad n^2 \text{ is even}\right)\text{"}$$

which has already been demonstrated to be true. So the original proposition is true □

2. Proof by Construction

Another method of proof is particularly useful for proving statements involving existential quantifiers (e.g., "there exists at least one ...").

This method works as follows:

In order to prove a statement of the form

"If *such and such*, then there exists an *object* such that *so and so*."

it suffices to construct (guess, produce, devise an algorithm to produce, etc.), using the hypothesis " *such and such*", the *object* in the conclusion and show that it satisfies the properties " *so and so*".

EXAMPLE 3.4. Prove that if $a < b$, then there exists a real number c such that

$$a < c < b \quad .$$

Proof. Set

$$c = \frac{a+b}{2} \quad .$$

Then

$$c - a = \frac{a+b-2a}{2} = \frac{b-a}{2} > 0$$

since $b > a$; and

$$b - c = \frac{2b-a-b}{2} = \frac{b-a}{2} > 0$$

for the same reason. Thus, we have constructed a number c with the desired properties.

EXAMPLE 3.5.

PROPOSITION 3.6. *If a, b, c, d, e and f are real numbers such that*

$$(ad - bc) \neq 0 \quad ,$$

then the two equations

$$\begin{aligned} ax + by &= e \\ cx + dy &= f \end{aligned}$$

can be solved for x and y.

proof. Our hypothesis is that a, b, c, d, e and f are real numbers such that

$$(ad - bc) \neq 0 \quad ,$$

and the conclusion we are trying to prove is that there exists real numbers x and y such that

$$\begin{aligned} ax + by &= e \quad , \\ cx + dy &= f \quad . \end{aligned} \tag{3.1}$$

Our basic plan is to apply a little high school algebra to construct a solution of the systems of equations. Thus, we might solve the first equation for y and then substitute the resulting expression for y into the second equation and solve for x. But note at that first step we end up with

$$y = \frac{e - ax}{b}$$

which requires an additional hypothesis, $b \neq 0$, which is distinct from our original hypothesis $ad - bc \neq 0$. This being the case, to get an air-tight proof, we'll need to handle the two cases $b \neq 0$ or $b = 0$ separately,

Case 1. $b \neq 0$. In this case, we can solve the first equation of y, to get

$$y = \frac{e - ax}{b}$$

Substituting this into the second equation we get

$$cx + d\left(\frac{e - ax}{b}\right) = f.$$

Multiplying this last equation by $-b$ we get

$$-cbx - de + adx = -fb$$

or

$$(ad - bc)\, x = de - fb$$

Since by hypothesis, $ad - bc \neq 0$, we can divide both sides by $ad - bc$ to get

$$x = \frac{de - fb}{ad - bc}$$

and then substituting this expression for x into our expression for y we get

$$y = \frac{af - ce}{ad - bc}$$

and so we arrive at a solution.

Case 2. If $b = 0$. In this situation, our equations specialize to

$$\begin{aligned} ax &= e \\ bx + dy &= f \end{aligned}$$

Now, also in this case, it must be that neither a or d equals zero; otherwise we will violate our hypothesis that $ad - bc \neq \dot{0}$. We can therefore solve the first equation for x

$$x = \frac{e}{a} \quad ,$$

Substituting this expression for x into the second equation, we get

$$dy = f - \frac{e}{a}$$

Since $d \neq 0$ in this case, we can obtain

$$y = \frac{1}{d}\left(f - \frac{e}{a}\right)$$

and we have a solution for this case.

Since Case 1 and Case 2 exhaust all possibilities (for b), our proof is complete $\square$