MATH 135 Fall 2006

Proofs, Part IV

We've spent a couple of days looking at one particular technique of proof: induction.
Let's look at a few more.

Direct Proof
Here we start with what we're given and proceed in a direct line to the conclusion.

Example
If n is an odd integer, then $n^2 - 1$ is divisible by 4.

Proof
Recall that every even integer can be written as $2m$ for some integer m and every odd integer can be written as $2k + 1$ for some integer k.
Since n is odd, $n = 2k + 1$ for some $k \in \mathbb{Z}$.
Thus

$$n^2 - 1 = (2k + 1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k^2 + 4k = 4(k^2 + k)$$

so is divisible by 4.

Tips

1) Most steps should be justified, with the exception of straightforward algebraic steps.
2) Always introduce/define new variables and give their domain.
3) Start with what you're given, not with what you want to prove.
4) Keep one eye forward and one behind; always be aware of where you're going.

Example
If a, b, c form an arithmetic sequence, then $(b - c)x^2 + (c - a)x + (a - b) = 0$ has equal roots.

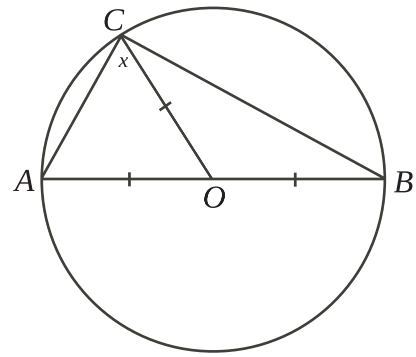
Proof
Since a, b, c form an arithmetic sequence, then $b = a + d$, $c = a + 2d$ for some $d \in \mathbb{R}$.
Thus our equation is

$$\begin{aligned} -dx^2 + 2dx - d &= 0 \\ -d(x^2 - 2x + 1) &= 0 \\ -d(x - 1)^2 &= 0 \end{aligned}$$

and so has two equal roots.

Example
If AB is a diameter of a circle and C is on the circle, then $\angle ACB = \frac{\pi}{2}$.

Proof



Let O be the centre of the circle and join CA, CO, and CB.
Suppose $\angle ACO = x$.
Since AO, BO and CO are radii, then $AO = BO = CO$.
Since $AO = CO$, then $\triangle ACO$ is isosceles, so $\angle CAO = \angle ACO = x$.
Therefore, $\angle COA = \pi - \angle ACO - \angle CAO = \pi - 2x$.
Also, $\angle COB = \pi - \angle COA = \pi - (\pi - 2x) = 2x$.
Since $CO = BO$, then $\triangle BCO$ is isosceles, so $\angle BCO = \angle CBO$.
Thus, looking at the angles in $\triangle COB$, $2x + 2\angle BCO = \pi$, so $\angle BCO = \frac{\pi}{2} - x$.
Therefore, $\angle ACB = \angle ACO + \angle BCO = x + \frac{\pi}{2} - x = \frac{\pi}{2}$, as required.

Compound Statements

If A and B are mathematical statements, we often see compound statements such as

"A and B" "A or B"

For "A and B" to be TRUE, both A and B must be TRUE.
Otherwise (when one is FALSE or both are FALSE), "A and B" is FALSE.
For "A or B" to be TRUE, either or both of A and B must be TRUE.
Otherwise (when both are FALSE), "A or B" is FALSE.

Example

$A =$"2 is a prime number", $B =$"5 is a perfect square"
Is "A and B" TRUE or FALSE?
Is "A or B" TRUE or FALSE?

Aside Regarding Sets

Recall that if A and B are sets, then $A \cup B$ is the set of elements that are in either A or B, and $A \cap B$ is the set of elements that are in both A and B.
So $A \cup B$ is similar to "A or B", and $A \cap B$ is similar to "A and B".

Example

If $A = \{1, 2, 4, 5, 6, 9, 10\}$ and $B = \{2, 3, 6, 7, 8\}$, then

$$\begin{aligned} A \cup B &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \\ A \cap B &= \{2, 6\} \end{aligned}$$

Converse Statements

Recall that a conditional statement is one of the form $A \Rightarrow B$ (ie. "If A then B").
The converse of such a statement is $B \Rightarrow A$ ("If B then A").

Example

"If the units digit of n is 5, then n is divisible by 5." (TRUE or FALSE?)
Converse: "If n is divisible by 5, then the units digit of n is 5." (TRUE or FALSE?)

"If n and $n + 1$ are both prime numbers, then $n = 2$." (TRUE or FALSE?)
Converse: "If $n = 2$, then n and $n + 1$ are both primes." (TRUE or FALSE?)

So there is no connection between the truth of a statement and its converse.

If and only if

In mathematics, we often see statements of the form "A if and only if B" ($A \Leftrightarrow B$)
This means "(If A then B) and (If B then A)". The parentheses are here for mathematical reasons, not English language ones!

Sometimes we say "(The truth of) A is equivalent to (the truth of) B" since if $A \Leftrightarrow B$ has been proven then if A is TRUE, B is TRUE, and if A is FALSE, B cannot be TRUE (otherwise A would be).

To prove these statements, we have two directions to prove, since there are two implications that must be proven to be TRUE.

Example

Suppose $x, y \geq 0$. Then $x = y$ if and only if $\dfrac{x+y}{2} = \sqrt{xy}$.

Proof

"$\Rightarrow$"

If $x = y \geq 0$, then $\dfrac{x+y}{2} = \dfrac{2x}{2} = x$ and $\sqrt{xy} = \sqrt{x^2} = x$ (since $x \geq 0$) so $\dfrac{x+y}{2} = \sqrt{xy}$.

"$\Leftarrow$"

If $\dfrac{x+y}{2} = \sqrt{xy}$, then

$$\begin{aligned}
x + y &= 2\sqrt{xy} \\
(x+y)^2 &= 4xy \\
x^2 + 2xy + y^2 &= 4xy \\
x^2 - 2xy + y^2 &= 0 \\
(x-y)^2 &= 0 \\
x &= y
\end{aligned}$$

Therefore, $x = y$ if and only if $\dfrac{x+y}{2} = \sqrt{xy}$.

Example

In $\triangle ABC$, $b = c\cos A$ if and only if $\angle C = 90°$.

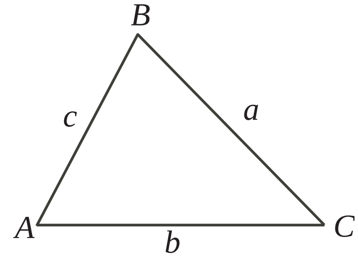
Proof

"$\Leftarrow$"

If $\angle C = 90°$, then $\cos A = \dfrac{b}{c}$, so $b = c\cos A$.

"$\Rightarrow$"

Suppose $b = c\cos A$.
Drop a perpendicular from B to P on AC.
Then $AP = AB\cos A = c\cos A$.
But $AC = AP + PC$ and $AC = b = c\cos A = AP$.
(Think about whether this makes sense if P is *to the right* of C.)
Thus $PC = 0$, so P and C coincide.
Therefore $\angle BCA = \angle BPA = 90°$.



Proof by Contradiction

Also sometimes called Indirect Proof or Reductio ad absurdum.
Here we list all possibilities including the one that is to be proved and show that all of the "other" possibilities lead to contradictions.

Example
Show that $\sqrt{2}$ is irrational.

Proof
Suppose that $\sqrt{2}$ is rational.

Aside The rational numbers are $\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0 \right\}$

Then $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$, $b \neq 0$, with a, b having no common factors.
Thus $a = \sqrt{2}b$ or $a^2 = 2b^2$.
Since the RS is even, the LS is even.
Since a^2 is even, then a is even, ie. $a = 2A$ for some $A \in \mathbb{Z}$.
Thus $4A^2 = 2b^2$ so $b^2 = 2A^2$.
Using a similar argument, b is even.
Therefore a and b have a common factor of 2, a contradiction.
Therefore $\sqrt{2}$ must be irrational.

Note
There are varying degrees of irrationality – if you're curious, check out algebraic and transcendental numbers.

Example
If $n + 1$ objects are to placed in n boxes, then there exists one box which will contain at least two objects.

Proof
Suppose that there is not such a box.
Then each of the n boxes contains at most one object.
Thus, the total number of objects is at most $1 \times n = n$, a contradiction.
Therefore there is one box which contains at least two objects.

> **Aside**
> This is the second proof of this result that we have seen.
> (See Proofs, Part 3 for the other one.)
> Which do you like better?
> Question: Do you think that this proof uses induction without saying so? If so, how?

Proof by Contrapositive

Recall that a statement $A \Rightarrow B$ has a converse $B \Rightarrow A$ which may or may not be TRUE when $A \Rightarrow B$ is TRUE.
$A \Rightarrow B$ also has a contrapositive (NOT B) $\Rightarrow$ (NOT A), i.e. "If B is not TRUE, then A is not TRUE."

Contrapositive Law
$A \Rightarrow B$ and (NOT B) $\Rightarrow$ (NOT A) are either both TRUE or both FALSE.

Consequence: If we can prove (NOT B) $\Rightarrow$ (NOT A), this is the same as proving $A \Rightarrow B$.

Justification
Suppose (NOT B) $\Rightarrow$ (NOT A) has been proven; and suppose that A is TRUE. Why is B TRUE?

Since A is TRUE, then NOT A is FALSE, so NOT B couldn't be TRUE (otherwise NOT A would be TRUE).
Therefore NOT B is FALSE so B is TRUE.
Therefore $A \Rightarrow B$ is TRUE.

Example
Prove that if x is a real number such that $x^4 + 7x < 9$, then $x < 1.1$.

Proof
We prove the contrapositive: "If $x \geq 1.1$, then $x^4 + 7x \geq 9$"
Since $x \geq 1.1$, then

$$x^4 + 7x \geq (1.1)^4 + 7(1.1) = 1.4641 + 7.7 = 9.1641$$

So the contrapositive is TRUE.
Therefore if $x^4 + 7x < 9$, then $x < 1.1$.

Example
Prove that if $a, b \in \mathbb{R}$ and ab is irrational, then a is irrational or b is irrational.

Proof
We prove the contrapositive: "If a is rational and b is rational, then ab is rational."

> **Aside**
> "NOT (A or B)" is "(NOT A) and (NOT B)"
> (If it is not TRUE that "A or B" is TRUE, then both A and B must not be TRUE.)
> Similarly, "NOT (A and B)" is "(NOT A) or (NOT B)".

If a and b are rational, $a = \dfrac{p}{q}$ and $b = \dfrac{m}{n}$ for some $m, n, p, q \in \mathbb{Z}$, $n, q \neq 0$.
Thus $ab = \dfrac{pm}{qn}$ which is rational.
This proves the contrapositive.

Note
The contrapositive is useful when it is difficult to get a handle on the hypotheses and conclusions of the original statement, but easier to deal with their negations.

Question
How do we know when to use what? Practice and intuition.

Quantifiers
There are two additional symbols to discuss: $\forall, \exists$.
Let $P(x)$ be a statement depending on x.
Then

- $\forall x$, $P(x)$ is "For all x, $P(x)$ is TRUE".
- $\exists x$, $P(x)$ is "There exists an x such that $P(x)$ is TRUE".

One catch: We need to specify the "universe of discourse" (that is, the domain) for x.

Example

Suppose $P(x) =$ "$x^2 = 2$"

Is $\forall x,\ P(x)$ TRUE or FALSE?

If U of D $= \{\sqrt{2}, -\sqrt{2}\}$, it is TRUE.

If U of D $= \mathbb{R}$, it is FALSE.

Is $\exists x,\ P(x)$ TRUE or FALSE?

If U of D $= \mathbb{Z}$, it is FALSE.

If U of D $= \mathbb{C}$, it is TRUE.

Note

The order of quantifiers matters.

Example

U of D is $\mathbb{R}$

$\forall x \exists y,\ x^3 - y^3 = 1$

"For all real numbers x, there exists a real number y such that $x^3 - y^3 = 1$."

(TRUE: for any x, we can solve for y.)

$\exists y \forall x,\ x^3 - y^3 = 1$

"There exists a real number y such that for all real numbers x, $x^3 - y^3 = 1$."

(FALSE: there is no single value of y that works for all x.)

Example

U of $D = \mathbb{Z}$

$\forall x \exists y,\ y \geq x$

"For all integers x, there exists a larger integer y"

$\exists y \forall x,\ y \geq x$

"There exists an integer y such that $y \geq x$ for all integers x."

Negations

NOT $(\forall x,\ P(x))$ $=$ $\exists x$, NOT $P(x)$

"It is not true that for all x, $P(x)$ is true." "There exists an x such that $P(x)$ is not true."

NOT $(\exists x,\ P(x))$ $=$ $\forall x$, NOT $P(x)$

Why do we care about quantifiers?

In mathematics, precision is very important. By its very nature, the English language is not very precise. Quantifiers are a way to translate statements in English that may or may not present ambiguities into precise mathematical statements, allowing us to agree on exactly what is being stated.

Example

Does the statement "$f(n) = 0$, where n is a positive integer" mean "$\forall n, f(n) = 0$" or does it mean "$\exists n, f(n) = 0$" (U of D is $\mathbb{P}$)? This is not clear. Translating to quantifiers can help us decide which we really mean.

That being said, translating from plain English to quantifiers can be difficult, as most of us normally do not use "for all" and "there exists" in everyday speech.

Examples

"There is always some number x with $x + y = 1$, no matter what number y is"

is really saying "For all numbers y, there exists a number x such that $x + y = 1$"

or $\forall y \exists x, x + y = 1$

"Some real numbers are not the square root of any real number"
is really saying
"There exists a real number x such for all real numbers y, x is not the square root of y"
or $\exists x \forall y, x \neq \sqrt{y}$

The best approach to these problems is to try to rewrite the English first into a more precise-looking form, and then convert to quantifiers.

Note
If we go back to the third Example in the Quantifiers section, the first statement could be written as "There is no largest integer" and the second statement could be written as "There is a largest integer".

One Final Note on Proofs

It is important when writing proofs not to start with what we want to prove and work in the wrong direction to get something that we know is true. (However, this "wrong" direction might in fact be the direction in which we figure out the proof.)

Example
Prove that if x, $y \in \mathbb{R}^+$ with $x - y \geq 1$ then $\frac{x}{y} + \frac{y}{x} \geq \frac{1}{xy} + 2$.
Rough Work

$$\begin{aligned}
\frac{x}{y} + \frac{y}{x} &\geq \frac{1}{xy} + 2 \\
x^2 + y^2 &\geq 1 + 2xy \\
x^2 - 2xy + y^2 &\geq 1 \\
(x-y)^2 &\geq 1 \\
x - y &\geq 1
\end{aligned}$$

The last step doesn't actually work in this direction, but this does allow us to figure out how to do this, as the steps all work in the other direction!

Proof

$$\begin{aligned}
x - y &\geq 1 \\
(x-y)^2 &\geq 1 \\
x^2 - 2xy + y^2 &\geq 1 \\
x^2 + y^2 &\geq 1 + 2xy \\
\frac{x}{y} + \frac{y}{x} &\geq \frac{1}{xy} + 2
\end{aligned}$$

as required.

It would be difficult to simply write out in this direction (it seems like magic), but with some work before, it can be done.