9/28

<u>Proofs by contrapositive</u> §2.2

Recall that many theorems are of the form $\forall x\ P(x) \to Q(x)$.
A proof by <u>contrapositive</u> of this theorem proves $\forall x\ \neg Q(x) \to \neg P(x)$, which is logically equivalent.

Proof by contrapositive can be useful when it is not clear how to "use" the hypothesis $P(x)$.

<u>E.g.</u> <u>Thm</u> for any two real numbers x, y, if $x+y \geq 2$ then $x \geq 1$ or $y \geq 1$.

<u>Pf.</u> A direct proof that $x+y \geq 2$ implies $x \geq 1$ or $y \geq 1$ looks challenging because it's not clear how to "use" the hypothesis $x+y \geq 2$. So let's try a proof by contrapositive. Thus, we need to show for all real numbers x, y, if not ($x \geq 1$ or $y \geq 1$) then not ($x+y \geq 2$).
So assume not ($x \geq 1$ or $y \geq 1$). Logically, by De Morgan's Law, this is equivalent to $x < 1$ and $y < 1$.
Then, we can use rules of inequalities to sum these inequalities to get $x+y < 2$. But $x+y < 2$ is exactly the same as not ($x+y \geq 2$), which is just what we wanted to prove. ∎

Even though $P(x) \to Q(x)$ and $\neg Q(x) \to \neg P(x)$ are logically equivalent, it can be helpful sometimes to start with the hypothesis $\neg Q(x)$ instead of the hypothesis $P(x)$. It's always worthwhile to consider if proof by contrapositive can be easier than a <u>direct proof</u>.

Proof by contradiction:

We will now discuss a very powerful proof strategy that is quite different from direct proof: proof by contradiction a.k.a. indirect proof.

A contradiction is a proposition which must be false, i.e., which logically cannot be true. More formally, a contradiction is a proposition of the form $r \vee \neg r$ for any proposition r.

Recall that a direct proof of $p \to q$ starts by assuming the hypothesis p and derives conclusion q. The way a proof by contradiction works is instead by assuming both the hypothesis p and the negation of the conclusion $\neg q$, and then derives a contradiction from these assumptions. This means that these assumptions could not be true, so that $p \wedge \neg q$ is false, i.e., $p \to q$ is true.

It's easiest to understand proof by contradiction by seeing some examples so let us do some:

E.g. Thm For every integer n, if n^2 is even then n is even.

First let's think about what a direct proof of this theorem might look like. We would start by assuming the hypothesis that n^2 is even, meaning $n^2 = 2k$, for

Some integer k_1. Then we want to conclude that n is even, i.e., that $n = 2k_2$ for some other integer k_2. But it does not seem clear how to find this k_2 in terms of k_1 (we cannot just "take square root"). So instead...

Pf by contradiction of thm: Let n be an integer. Assume, by way of contradiction, that n^2 is even but n is not even. Since n is not even, it is odd, meaning $n = 2k+1$ for some integer k.

Then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$
$$= 2(2k^2 + 2k) + 1.$$
But this means n^2 is odd (since $2k^2+2k$ is an integer). That's a contradiction, since we assumed n^2 is even. So our assumptions must have been false. Thus, it cannot be that n^2 is even and n is odd at the same time; so if n^2 is even then n must be even. This is exactly what we wanted to prove! $\boxtimes$

Let's see another famous example of a theorem that's easiest to prove by contradiction.

10/7 Theorem The number $\sqrt{2}$ is irrational.
(Recall that a number x is rational if $x = p/q$ where p and q are integers.)

A direct proof of this theorem looks unpromising: all we are given is the number $x = \sqrt{2}$, which satisfies the properties $x^2 = 2$ and $x > 0$. Unclear how this relates to rationality.

Pf by contradiction that $\sqrt{2}$ is irrational:

Assume by way of contradiction that $\sqrt{2}$ is rational. Thus we can write $\sqrt{2} = \frac{p}{q}$ for integers p and q, and by writing this expression is in "lowest terms" (i.e., we canceled all common factors) we can assume that p and q are not both even. Then by squaring we get $2 = \frac{p^2}{q^2}$ i.e. $2q^2 = p^2$. So p^2 is even. It follows from thm we just proved that p is even, i.e., there is k such that $p = 2k$. Substituting, this means $2q^2 = (2k)^2 = 4k^2$, so $q^2 = 2k^2$. Thus q^2, and therefore q, are even. But this contradicts our assumption that p and q were not both even. So we conclude $\sqrt{2}$ is irrational. ☒

Exercise: Use proof by contradiction to show that $\forall$ real numbers x, y, if $x+y \geq 2$ then $x \geq 1$ or $y \geq 1$.

We proved this before using contraposition. You may notice proof by contrapositive and proof by contradiction seem similar. Indeed, showing the contrapositive $\neg q \to \neg p$ is formally the same as showing that $p \wedge \neg q$ leads to a contradiction. So often it is just a matter of taste whether one prefers to phrase an argument as proof by contradiction or proof by contrapositive. //

10/12

Mathematical Induction § 2.4

Suppose we have a sequence of circles in a row:

1 2 3 4 ...

where the circles are numbered 1, 2, 3, ... left-to-right.

Suppose we know that
- Circle 1 is colored red,
- If circle n is colored red, then circle $n+1$ is colored red, for all $n \geq 1$.

Then we can conclude that all the circles are colored red. This kind of reasoning is called (mathematical) induction, and it is a very powerful technique for proving theorems.

Let's show a more mathematical use of induction:

Thm for any positive integer n,

$$1+2+3+\cdots+n = \frac{n(n+1)}{2}.$$

Pf: First, notice that it is true for $n=1$

$$\frac{1(1+1)}{2} = 1 \cdot \frac{2}{2} = 1 \checkmark$$

Then, assume it is true for n, i.e.,

$$1+2+\cdots+n = \frac{n(n+1)}{2}.$$

Let's show that it is true for $n+1$: by our assumption,

$$\begin{aligned} 1+2+\cdots+n+(n+1) &= \frac{n(n+1)}{2} + n+1 \\ &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{(n+2)(n+1)}{2} = \frac{(n+1)((n+1)+1)}{2}, \end{aligned}$$

which is exactly the statement of the theorem for $n+1$.

By the principle of mathematical induction, the theorem is proved. $\boxtimes$

What is the principle of (mathematical) induction?

It says that if $P(n)$ is a propositional formula whose domain of discourse is the set $\{1, 2, 3, \dots\}$ of positive integers such that:

- $P(1)$ is true
- if $P(n)$ is true then $P(n+1)$ is true, for all $n \in \{1, 2, 3, \dots\}$

Then: $P(n)$ is true for all $n \in \{1, 2, 3, \dots\}$.

Why is the principle of induction correct?

Well, to show $P(n)$ is true for some fixed $n \in \{1, 2, 3, \dots\}$ we can reason as follows:

- $P(1)$ is true
- If $P(1)$ is true then $P(2)$ is true.
- If $P(2)$ is true then $P(3)$ is true

$\vdots$

- If $P(n-1)$ is true then $P(n)$ is true.

$\therefore$ $P(n)$ is true.

See how we made a "chain" of if...then's connecting the "$P(1)$ is true" assumption to "$P(n)$ is true."

In a proof by induction, the statement "$P(1)$ is true" is called the base case (or "basis step") and the statement "$\forall n$, If $P(n)$ then $P(n+1)$" is called the inductive step. It is very important to establish both the base case and the inductive step to have a valid proof by induction!

10/14

Let's see some more proofs by induction:

<u>Thm</u> The number of subsets of $\{1,2,\dots,n\}$ is 2^n.

<u>Pf:</u> We prove by induction. The base case $n=1$ is correct since there are two subsets: $\emptyset$ and $\{1\}$. Now assume that # of subsets of $\{1,2,\dots,n\}$ is 2^n for some $n \geq 1$. We must show # subsets of $\{1,2,\dots,n+1\}$ is 2^{n+1}, i.e., there are twice as many subsets of $\{1,2,\dots,n+1\}$ as of $\{1,2,\dots,n\}$. To prove this, notice for every subset $S \subseteq \{1,2,\dots,n\}$ we can make two subsets of $\{1,2,\dots,n+1\}$: S itself, and $S \cup \{n+1\}$. And each subset of $\{1,2,\dots,n+1\}$ is made in a unique way this way. So by induction we are done! $\blacksquare$

Theorem For all $n \geq 1$, $n! \geq 2^{n-1}$, where <u>n factorial</u> is $n! = n \times (n-1) \times (n-2) \times \cdots \times 3 \times 2 \times 1$.

<u>Pf:</u> The base case $n=1$ is ok since $1! = 1 = 2^0 = 2^{1-1}$. So now assume for some $n \geq 1$ that $n! \geq 2^{n-1}$.

Then
$$\begin{aligned}
(n+1)! &= (n+1) \times n! && \text{(from def. of factorial)} \\
&\geq (n+1) \times 2^{n-1} && \text{(by induction)} \\
&\geq 2 \times 2^{n-1} && \text{(since } n+1 \geq 2 \text{ since } n \geq 1\text{)} \\
&= 2^n.
\end{aligned}$$

Thus we proved the statement for $n+1$, and so by induction it is true. $\blacksquare$