2/24 <u>Indirect proofs</u> §2.2

We now learn proof techniques <u>beyond</u> direct proofs.

<u>Proof by contrapositive</u>: Recall most theorems are of form $\forall x\, P(x) \to Q(x)$. A <u>proof by contrapositive</u> of this theorem proves $\forall x\, \neg Q(x) \to \neg P(x)$, which is logically equivalent but can sometimes be easier when we don't see how to "use" hypothesis $P(x)$.

<u>E.g.</u> <u>Thm</u> For real numbers x and 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 that $x+y \geq 2$. So let's try a proof by contrapositive instead. Thus, we need to show for all real numbers x and y, if not $(x \geq 1$ or $y \geq 1)$ then not $(x+y \geq 2)$. So assume x, y satisfy not $(x \geq 1$ or $y \geq 1)$. By De Morgan's Laws, this is equivalent to $x < 1$ and $y < 1$. Summing these inequalities gives $x+y < 2$. But $x+y<2$ is same as not $(x+y \geq 2)$, which is exactly what we were trying to prove. $\boxtimes$

We see how even though $P(x) \to Q(x)$ and $\neg Q(x) \to \neg P(x)$ are log. equivalent, sometimes easier to start with $\neg Q(x)$ than with $P(x)$. "Solving <u>a maze backwards</u>."

<u>Proof by contradiction</u>: Proof by contradiction is another, very powerful "indirect" proof technique that is quite similar to proof by contrapositive. Main idea behind proof by contradiction: you start by assuming the <u>opposite</u> of what you wish to prove, and use that to reach a <u>contradiction</u>.

A contradiction is a proposition which must be false, i.e., one which logically can never be true. More formally, a contradiction is a proposition of the form $r \wedge \neg r$ for any proposition r.

Recall that a direct proof of $p \to q$ starts by assuming the hypothesis p and then 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 the assumptions could not be true, so that $p \wedge \neg q$ is false. But $p \wedge \neg q$ being false exactly means $p \to q$ is true.

It's easiest to understand proof by contradiction by seeing how it works in some examples:

E.g. Thm For all integers n, if n^2 is even then n is even.

First let us think about what a direct proof of this theorem might look like. We would start by assuming that n^2 is even, meaning that $n^2 = 2 \cdot k_1$ for some integer k_1. Then we want to conclude that n itself is even, i.e. that $n = 2 \cdot k_2$ for some integer k_2. However, it does not seem very clear how to "find" this k_2 in terms of k_1 (we cannot just "take square roots.")

So instead of proving this theorem directly, let us try to give a proof by contradiction...

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, meaning that if n^2 is even then n must be even. This is precisely what we wanted to prove! ▨

2/27 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.

So instead, we will give a famous ...

Proof 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. By cancelling all common factors, we can assume furthermore that this expression is in "lowest terms," i.e., that there is no integer $n>1$ dividing both p and q.

(E.g. $\frac{8}{6} = \frac{4}{3}$ ← in lowest terms since nothing divides both 4 and 3)

In particular, we can assume that p and q are not <u>both</u> <u>even</u> (i.e., 2 does not divide both).

By squaring $\sqrt{2} = p/q$ we get that $2 = p^2/q^2$, i.e., that $2q^2 = p^2$. So p^2 is even.

It follows from the theorem we proved earlier that p <u>is</u> <u>even</u>, i.e., that $p = 2k$ for some integer k.

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 <u>not</u> both even. We conclude that $\sqrt{2}$ is irrational. ∎

We see in this last example how <u>proof by contradiction</u> can be employed even when the theorem is <u>not</u> of the form $\forall x \; P(x) \to Q(x)$.

<u>Exercise</u>: Use a proof by contradiction to show that for all real numbers x and y, if $x+y \geq 2$ then $x \geq 1$ or $y \geq 1$.

We proved this before using <u>contraposition</u>.

You may notice that proof by contradiction and proof by contrapositive 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 to phrase an argument as proof by contradiction or proof by contrapositive...

//

3/1 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 also 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's a very powerful technique for proving theorems.

Let's show a more mathematical use of induction:

Theorem 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 some $n \geq 1$, 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 $n+1$.

Therefore, by the principle of mathematical induction, the theorem is proved for all $n \geq 1$. ∎

So what is the principle of (mathematical) induction?

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

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

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

Why is the principle of induction correct?

Well, to show $P(n)$ is true for some fixed $n \in \{1,2,3,\ldots\}$ 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 "$P(1)$ is true" assumption to "$P(n)$ is true" conclusion.

In a proof by induction, the statement

- "$P(1)$ is true" is called the base case (or "basis step")

while 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 & the inductive step to give a valid proof by induction!

Let's see some more proofs by induction:

<u>Thm</u> $2^0+2^1+2^2+\cdots+2^{n-1}=2^n-1$ for any $n\geq 1$.

<u>Pf</u>: First we check the <u>base case</u> $n=1$:

$$2^0=1=2^1-1 \checkmark$$

Next, we do the <u>inductive step</u>. So assume formula for some (fixed) $n\geq 1$:

$$2^0+2^1+2^2+\cdots+2^{n-1}=2^n-1.$$

Then, for $n+1$ we have by our inductive assumption:

$$(2^0+2^1+\cdots+2^{n-1})+2^n=(2^n-1)+2^n$$
$$=2\cdot 2^n-1=2^{n+1}-1,$$

the correct formula for the case $n+1$. By induction, we're done! ☒

The kind of sum in this last theorem is called a <u>geometric sum</u>: See Example 2.4.4 in the textbook.

Also, notice a key part of these theorems is <u>guessing the correct formula</u> in terms of n.

3/13 We can also prove <u>inequalities</u> by induction:

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

<u>Pf</u>: The base case is good since $1!=1=2^0=2^{1-1}$ ✓

So now assume for some $n\geq 1$ that $n!\geq 2^{n-1}$.

Then $(n+1)! = (n+1)\times n!$ (from def. of factorial)

$\geq (n+1)\times 2^{n-1}$ (by inductive assumption)

$\geq 2\times 2^{n-1}$ (since $n\geq 1$ so $n+1\geq 2$)

$\geq 2^n$.

We proved the inequality in the case $n+1$, so by induction the theorem is true for all $n\geq 1$. ☒

Induction can be used for more than just formulas involving n:

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

Pf: We prove by induction. The base case $n=1$ is correct since there are two subsets: $\emptyset$ and $\{1\}$.
Now assume # of subsets of $\{1,2,\dots,n\}$ is 2^n for some $n\geq 1$.
We must show # of subsets of $\{1,2,\dots,n+1\}$ is 2^{n+1}, i.e., that there are twice as many subsets of $\{1,2,\dots,n+1\}$ as of $\{1,2,\dots,n\}$.
To prove this, notice that for every subset $S\subseteq\{1,2,\dots,n\}$ we can make two subsets of $\{1,2,\dots,n+1\}$: S and $S\cup\{n+1\}$

E.g. $n=1$: $\emptyset \to \emptyset$, $\emptyset \to \{2\} \subseteq \{1,2\}$; $\{1\} \to \{1\}$, $\{1\} \to \{1,2\}$

We get all subsets of $\{1,\dots,n+1\}$. So by induction, we are done! ∎

Strong form of Mathematical Induction §2.5

We can "strengthen" induction as follows: let $P(n)$ be a prop. formula with discourse domain $\{1,2,\dots\}$. Suppose that:

- $P(n_0)$ is true, $P(n_0+1)$ is true, $\dots$, $P(n_0+(m-1))$ is true for some $n_0\in\{1,2,\dots\}$ and some $m\geq 1$, (base cases)
- for all $n\geq n_0+(m-1)$, if $P(k)$ is true for all $n_0\leq k<n$, then $P(n)$ is true. (inductive step)

Then $P(n)$ is true for all $n\geq n_0$.

Notice how we allow multiple base cases, and the base cases don't have to start at $n=1$.
However, the main strength of strong induction is that when proving $P(n)$ we can assume $P(k)$ for all $k<n$, not just $n-1$.

Here are some examples of using strong induction:

Thm Using 2¢ and 5¢ stamps, for any amount $n \geq 4$ we can make postage worth n¢.

Pf: We use two base cases: $n = 4$¢ $= 2$¢ $+ 2$¢ and $n = 5$¢ (one 5¢ stamp). Then for $n \geq 6$: we know by the strong principle of induction that we can make $(n-2)$¢ postage, so just add 2¢ stamp to get n¢ postage. (Notice we needed $(n-2)$¢ not $(n-1)$¢). $\boxtimes$

The Fibonacci numbers F_n for $n \geq 1$ are defined by $F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$.

E.g.
$$F_3 = F_1 + F_2 = 1 + 1 = 2$$
$$F_4 = F_2 + F_3 = 1 + 2 = 3$$
$$F_5 = F_3 + F_4 = 2 + 3 = 5 \ldots$$

Thm $F_n \leq 2^{n-1}$ for all $n \geq 1$.

Pf: We use strong induction. Have two base cases:
$$n = 1 \rightsquigarrow F_1 = 1 \leq 2^0 = 2^{1-1} \checkmark$$
$$n = 2 \rightsquigarrow F_2 = 1 \leq 2^1 = 2^{2-1} \checkmark$$

Now, for $n > 2$, assume that $F_{n-1} \leq 2^{n-2}$ and $F_{n-2} \leq 2^{n-3}$ using strong induction.

Thus,
$$\begin{aligned} F_n &= F_{n-2} + F_{n-1} && \text{(by def. of Fibonacci \#'s)} \\ &\leq 2^{n-3} + 2^{n-2} && \text{(by induction)} \\ &\leq 2^{n-2} + 2^{n-2} = 2(2^{n-2}) = 2^{n-1}. \end{aligned}$$

and so by induction we are done! $\boxtimes$

See how strong induction is useful when we have recurrences that "go back" more than 1 step.