What is induction? It refers to two different definitions. One is about the composition of the set of natural numbers $\mathbb{N}$. The other is a method of proof of mathematical statements. Lets start by the first one.

Set of Natural Numbers

Definition: Set of Natural Numbers

The set of Natural Numbers is the smallest set such that,

- $0 \in \mathbb{N}$
- $n \in \mathbb{N} \to n+1 \in \mathbb{N}$

This definition contains 3 of the 5 ideas behind Peano axioms. They are,

- $0 \in \mathbb{N}$
- $n \in \mathbb{N} \to n+1 \in \mathbb{N}$
- $n+1 = 0 \to n \notin \mathbb{N}$
- $n+1 = m+1 \to n = m$
- $(0 \in A \wedge n \in A \to n+1 \in A) \to A \subseteq \mathbb{N}$

Proof by Induction

To prove a family of statements $\forall n \in \mathbb{N} \colon P(n)$, we can use proof by induction.

Definition: Principle of Mathematical Induction

By proving the *initial case* $P(0)$ and the *induction step* $P(k) \to P(k+1)$ we conclude $\forall n \in \mathbb{N} \colon P(n)$. Formally,

$$(P(0) \wedge P(k) \to P(k+1)) \to \forall n \in \mathbb{N} \colon P(n)$$

Example 1 Intro to Uni Math Sheet 1: Upper bounded sum and the lower bounded product

Let $x_1 + x_2 + \ldots + x_n \leq \frac{1}{3}$. Show that $(1-x_1)(1-x_2)\ldots(1-x_n) \geq \frac{2}{3}$

Doubt

What is the trick here?

Example : Sum of first n natural numbers

We want to prove the following,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Initial Case: n=1

$$\sum_{i=1}^{1} i = 1 = \frac{1(2)}{2}$$

$\square$

Induction step:

$$\left(\sum_{i=1}^{n} i = \frac{n(n+1)}{2}\right) \to \left(\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}\right)$$

To prove the induction step,

$$\begin{aligned}
\sum_{i=1}^{n+1} i &= (n+1) + \sum_{i=1}^{n} i && \text{Using the induction hypothesis we get} \\
&= (n+1) + \frac{n(n+1)}{2} \\
&= \frac{2n+2}{2} + \frac{n(n+1)}{2} \\
&= \frac{2n+2+n^2+n}{2} \\
&= \frac{n^2+3n+2}{2} \\
&= \frac{(n+1)(n+2)}{2}
\end{aligned}$$

□

We can also reduce the scope of the statement to a subset of natural numbers. Instead of the initial case being $P(0)$, we can start with the property $P(k)$ of a given natural number k.

Principle: Advice on proving a statement by Induction

Always try to decompose conclusion into induction hypothesis and other term.

Strong Induction

The induction hypothesis is now,

$$(P(0) \wedge P(1) \wedge \ldots \wedge P(k)) \to P(k+1)$$

Example University of Illinois: Proof Recurrence Relation by Strong Induction

Let a_n be a sequence where $a_1 = 1$ and $a_2 = 8$ and $a_n = a_{n-1} + 2a_{n-2}$. We want to prove that,

$$a_n = 3 \cdot 2^{n-1} + 2(-1)^n$$

We prove by induction on n. Initial case: $n = 3$

$$a_3 = 10$$

□

Inductive Step: $3 \leq n \leq k \to a_n = 3 \cdot 2^{n-1} + 2(-1)^n$

$$\begin{aligned} a_{n+1} &= a_n + 2a_{n-1} && \text{We can use the induction hypothesis twice} \\ &= 3 \cdot 2^{n-1} + 2(-1)^n + 2\left(3 \cdot 2^{n-2} + 2(-1)^{n-1}\right) \\ &= 2(3 \cdot 2^{n-1}) + 2(-1)^n + 2^2(-1)^{n-1} \\ &= 3 \cdot 2^n + 2(-1)^{n-1}(-1+2) \\ &= 3 \cdot 2^n + 2(-1)^{n-1} \\ &= 3 \cdot 2^n + 2(-1)^{n+1} \\ &\square \end{aligned}$$

Principle: Strong Induction

We notice that weak induction is not enough when we need more than a single hypothesis in the induction step.

Forward-Backward Induction

We have the same 2 steps in a regular proof by induction, the initial case and the inductive step, but the inductive step is composed by two different steps.

- Initial case: $P(0)$
- Inductive step:
  - Forward step: $P(k) \to P(f(k))$ where f is an increasing function.
  - Backward step: $P(k) \to P(k-1)$

Quest: More patterns in forward backward induction

Find an application of a proof that requires more than one forward and/or backward step. Example:

- $f_1(k) = 2^k$
- $f_2(k) = 2^k - 1$
- $b(k) = k - 2$

Example brilliant.org: AM-GM Inequality

Initial Case: $\frac{a+b}{2} \geq \sqrt{ab}$

$$\begin{aligned} (a-b)^2 \geq 0 \leftrightarrow \\ & a^2 - 2ab + b^2 \geq 0 \leftrightarrow \\ & a^2 + 2ab + b^2 - 4ab \geq 0 \leftrightarrow \\ & a^2 + 2ab + b^2 \geq 4ab \leftrightarrow \\ & a^2 + 2ab + b^2 \geq 4ab \leftrightarrow \\ & (a+b)^2 \geq 4ab \leftrightarrow \\ & |a+b| \geq 2\sqrt{ab} \leftrightarrow && \text{Since both a and b are positive so is their addition} \\ & \to a+b \geq 2\sqrt{ab} \\ & \to \frac{a+b}{2} \geq \sqrt{ab} \end{aligned}$$

Inductive Step:

Induction Hypothesis:

$$\frac{\sum_{i=1}^{k} a_i}{k} \geq \sqrt[k]{\prod_{i=1}^{k} a_i}$$

Forward pass: We want to show,

$$\frac{\sum_{i=1}^{2k} a_i}{2k} \geq \sqrt[2k]{\prod_{i=1}^{2k} a_i}$$

We can start by splitting the summation in the left hand side,

$$\begin{aligned}
a_1 + a_2 + \cdots + a_{2k} &= \frac{\frac{a_1+a_2+\cdots+a_k}{k} + \frac{a_{k+1}+a_{k+2}+\cdots+a_{2k}}{k}}{2} \\
&\geq \frac{\sqrt[k]{a_1 a_2 \cdots a_k} + \sqrt[k]{a_{k+1} a_{k+2} \cdots a_{2k}}}{2} \\
&\geq \sqrt{\sqrt[k]{a_1 a_2 \cdots a_k}\,\sqrt[k]{a_{k+1} a_{k+2} \cdots a_{2k}}} \\
&= \sqrt[2k]{a_1 a_2 \cdots a_{2k}}
\end{aligned}$$

$\square$

This completes the proof for the forward pass.

Backward pass: We want to show,

$$\frac{\sum_{i=1}^{k-1} a_i}{k-1} \geq \sqrt[k-1]{\prod_{i=1}^{k-1} a_i}$$

We start by using the inductive hypothesis,

$$\begin{aligned}
\frac{a_1 + a_2 + \cdots + a_k}{k} &\geq \sqrt[k]{a_1 a_2 \cdots a_k} \\
\frac{a_1 + a_2 + \cdots + a_{k-1} + \frac{a_1+a_2+\cdots+a_{k-1}}{k-1}}{k} &\geq \sqrt[k]{a_1 a_2 \cdots a_{k-1} \cdot \frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1}} && (*1) \\
\frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1} &\geq \sqrt[k]{a_1 a_2 \cdot \cdot a_{k-1} \cdot \frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1}} \\
\left(\frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1}\right)^k &\geq a_1 a_2 \cdots a_{k-1} \cdot \frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1} \\
\left(\frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1}\right)^{k-1} &\geq a_1 a_2 \cdots a_{k-1} \\
\frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1} &\geq \sqrt[k-1]{a_1 a_2 \cdots a_{k-1}}
\end{aligned}$$

$\square$

This completes the backward pass and the proof of the AM-GM Inequality.

(*1) The used property is: the arithmetic mean of k numbers in which one of them is the mean of the other $k-1$ numbers is actually the mean of the same $k-1$ numbers.

Double Induction

We start by defining the addition of two natural numbers recursively,

Definition: Recursive Definition of Addition of Two Natural Numbers

Let m and n be natural numbers.

- m+0=m
- m+(n+1)=(m+n)+1

Example Intro to Uni Math ex.2: Commutativity of Addition of Natural Numbers

We want to show that the addition is commutative using its recursive definition,

$$m + n = n + m$$

Let $n = 0$. We want to show that $m + 0 = 0 + m$. We show by induction on m. The base case is skipped. We assume $k + 0 = 0 + k$. We want to prove $0 + (k + 1) = (k + 1) + 0$

$$\begin{aligned}
0 + (k + 1) &= (0 + k) + 1 && \text{Recursive Part of Definition} \\
&= (k + 0) + 1 && \text{Inductive Hypothesis} \\
&= k + 1 && \text{Base Case for Recursive Definition LR} \\
&= (k + 1) + 0 && \text{Base Case for Recursive Definition RL}
\end{aligned}$$

Let $n = 1$. We want to show that $m + 1 = 1 + m$. We show by induction on m. Base case $0 + 1 = 1 + 0$ was already proven when $n = 0 \wedge m = 1$. We assume $k + 1 = 1 + k$. We want to prove $1 + (k + 1) = (k + 1) + 1$

$$\begin{aligned}
(k + 1) + 1 &= (1 + k) + 1 && \text{Inductive Hypothesis} \\
&= 1 + (k + 1) && \text{Recursive Part of Definition RL}
\end{aligned}$$

□

We want to show that $m + n = n + m$. We prove by induction on n. The base case was already shown. We assume $m + k = k + m$. We want to prove $m + (k + 1) = (k + 1) + m$

$$\begin{aligned}
(m + k) + 1 &= (k + m) + 1 && \text{Inductive Hypothesis} \\
&= 1 + (k + m) && \text{Using (ii)} \\
&= (1 + k) + m && \text{Recursive Part of Definition} \\
&= (k + 1) + m && \text{Using (ii)}
\end{aligned}$$

□

Example 3 Intro to Uni Math, Sheet 1: Every integer has an unique expansion in base b

Show that every integer $x \geq 1$ and for a base $b \geq 2$ has an unique expansion with the following form,

$$x = a_0 b^0 + a_1 b^1 + a_2 b^2 + \dots$$

We start by proving the existence of an expansion for every integer $x \geq 1$ by forward-backward induction.

Existence The initial case consists of proving the existence of a representation for $x = 1$.

$$x = 1b^0$$

□

The inductive step is divided into two different proofs, one for the forward pass and another for the backward one.

Forward pass: $P(k) \to P(b^k)$

$$b^k = b^k + \sum_{i=0}^{k-1} 0b^i$$

Backward pass: $P(k) \to P(k-1)$

The coefficients of the predecessor $k-1$ are noted as c_i, where j is the index of the first non-zero coefficient.

$$c_i = \begin{cases} b-1 & , \ i < j \\ c_i - 1 & , \ i = j \\ c_i & , \ i > j \end{cases}$$

This concludes the proof of the backward pass and the proof of existence of an expansion for every integer in base b.

Uniqueness This part of the proposition is proved by contradiction where we show that for the minimum integer that has more than one expansion in base b, that we can build smaller integers that also have more than one expansion.

Lets assume that this integer is w and that the two different representations are the following,

$$\begin{aligned} w &= (a_0, a_1, \ldots, a_i, \ldots, a_n) \\ &= (c_0, c_1, \ldots, c_i, \ldots, c_n) \end{aligned}$$

Let i be the index of the first different entry such that $a_i \neq c_i$. We can also assume that if $i \neq 0$ then every other coefficient must be zero because if it weren't then we could build a smaller integer that also had two different representations. If we can make this assumption, then we can try to describe the coefficients of the predecessor $w-1$. Lets assume that $c_i - a_i > 0$ and that $a_i \neq 0$

$$\begin{aligned} w - 1 &= (b-1, b-1, \ldots, a_i - 1, \ldots, a_n) \\ &= (b-1, b-1, \ldots, c_i - 1, \ldots, c_n) \end{aligned}$$

We can set the coefficients before i to zero so that we have a smaller integer with more than one expansion in base b. In the case that $a_i = 0$, the ith position would have $b-1$ in the first representation and since $c_i - 1$ is upper bounded by $b-2$, we can still build a smaller integer that has two different representations. In the case of $i = 0$ then the first coefficient of the predecessor $w-1$ is going to have at least two different expansions since the first representation would have either $a_i - 1$ and the second $c_i - 1$ (and they are different) or the first would have $b-1$ and the second would be upper bounded by $b-2$.

[Really confusing this last part of the proof! Ask for help!]

Infinite Descent

Example Wikipedia: Proof by Infinite Descent

The square root of a non-integer is always irrational, formally,

$$k \notin \mathbb{N} \to \sqrt{k} \notin \mathbb{R} - \mathbb{Q}$$

Let $\sqrt{k}$ be a rational number and q the last integer before $\sqrt{k}$,

$$\begin{gathered} \sqrt{k} \in \mathbb{Q} \leftrightarrow \sqrt{k} = \frac{m}{n}, \ m, n \in \mathbb{N} \\ q \in \mathbb{N} \land q < \sqrt{k} \land q + 1 > \sqrt{k} \end{gathered}$$

We start by describing k,

$$\begin{aligned}\sqrt{k} &= \frac{m}{n} \\ &= \frac{m(\sqrt{k}-q)}{n(\sqrt{k}-q)} \\ &= \frac{m\sqrt{k}-mq}{n\sqrt{k}-nq} \qquad (*2) \\ &= \frac{n\sqrt{k}\sqrt{k}-mq}{n\frac{m}{n}-nq} \\ &= \frac{nk-mq}{m-nq} \\ &\square\end{aligned}$$

Since there is an irreducible fraction for every rational number then the last expression is a contraction.

(*2) We want to get rid of $\sqrt{k}$ so we have to try to replace either the square itself or the term multiplying by the square root.

Structural Induction

The power set of a set A, $\mathbb{P}(A)$, can be defined recursively.

Definition: Power Set

Let A be a set. The smallest set that satisfies the properties below is the power set of A. An equivalent definition is that the power set is composed by all the subsets of A.

- $\emptyset \in \mathbb{P}(A)$
- $B \in \mathbb{P}(A) \wedge x \in A \leftrightarrow B \cup \{x\} \in \mathbb{P}(A)$

Doubt

NEED HELP! Is the definition OK? Should probably prove the equivalence. Does the previous definition qualify as a recursive one?

Tricks

TODO