

Induction

Properties. A property of natural numbers is a function from the natural numbers to $\{T, F\}$.

Examples

- Being odd: Define $odd(n)$ to mean that natural number n is odd
- Being prime: Define $prime(n)$ to mean that n is prime
- Triangular sum. Define $tri(n)$ to mean

$$\left(\sum_{i=0}^{n} i\right) = \frac{n(n+1)}{2}$$

Of these odd and $prime$ are not true of all natural numbers, but tri is true of all natural numbers

- $\neg\forall n \in \mathbb{N}, odd(n)$
- $\neg\forall n \in \mathbb{N}, prime(n)$
- $\forall n \in \mathbb{N}, tri(n)$

Simple Induction

Suppose we know for a property P of the natural numbers that: If

- (a) P is true of 0.
- (b) that for all k in $\mathbb{N}$, if the property is true of k, then it is also true of $k+1$.
  - ∗ I.e. $(P(0) \to P(1))$ and $(P(1) \to P(2))$ and $(P(2) \to P(3))$ and ...

Then

- From (a) we know $P(0)$ is true
- From $(P(0) \to P(1))$ and $P(0)$, we know $P(1)$ is true
- From $(P(1) \to P(2))$ and $P(1)$, we know $P(2)$ is true
- From $(P(2) \to P(3))$ and $P(2)$, we know $P(3)$ is true
- and so on ad infinitum.

In fact it must be that $P(n)$ is true for all $n \in \mathbb{N}$.

Example 0

Consider the property of n that $\left(\sum_{i=0}^{n} i\right) = \frac{n(n+1)}{2}$.

- (a) We define
$$tri(n) \text{ iff } \left(\sum_{i=0}^{n} i\right) = \frac{n(n+1)}{2}$$
- (b) (Base Step) We will show $tri(0)$
- (d) (Induction Step) We will show that, for any k in $\mathbb{N}$, if $tri(k)$, then $tri(k+1)$

- Now we have
  - $tri(0)$ by the base step
  - $tri(1)$ by the induction step and $tri(0)$
  - $tri(2)$ by the induction step and $tri(1)$
  - and so on
- In fact we have $\forall n \in \mathbb{N}, tri(n)$. That is

$$\forall n \in \mathbb{N}, \left(\sum_{i=0}^{n} i \right) = \frac{n(n+1)}{2}$$

The Theorem of Mathematical Induction

Principle: The *“theorem of (simple) mathematical induction”* states that

Notes

- The antecedent $P(k)$ is called the “induction hypothesis” (Ind. Hyp.)
- Proof is based on the WOP. See book.
- In applying this theorem
  - $P(0)$ is called the “base step”
  - $\forall k \in \mathbb{N}, P(k) \rightarrow P(k+1)$ is called the “inductive step”

Informal “proof”: Recall that $P \wedge Q \Leftrightarrow P \wedge (P \rightarrow Q)$

- In the infinite case we have

$$\begin{aligned} & P(0) \wedge P(1) \wedge P(2) \wedge \cdots \\ \Leftrightarrow\ & P(0) \wedge (P(0) \rightarrow P(1)) \wedge (P(1) \rightarrow P(2)) \wedge \cdots \end{aligned}$$

A proof by the theorem of (simple) mathematical induction answers the following questions

- (a) What is the property of the natural numbers?
- (b) What do we need to prove for the base step?
- (c) What is a proof of the base step?
- (d) What do we need to prove for the inductive step?
- (e) What is a proof of the inductive step?

Example 1

We will show that, for all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i^2 = n(n+1)(2n+1)/6$$

Proof:

(a) Let $P(n)$ be the property of a natural number n that $\sum_{i=1}^{n} i^2 = n(n+1)(2n+1)/6$

- (b) *Base Step:* We need to show $P(0)$,i.e.

$$\sum_{i=1}^{0} i^2 = 0(0+1)(0n+1)/6$$

  - ∗ (c) *Proof of Base Step:* The LHS is 0 since the sum of 0 things is always 0. The RHS simplifies to 0. Thus $P(0)$ holds.

- (d) *Induction Step.* We need to show that $\forall k \in \mathbb{N}$, if

$$\sum_{i=1}^{k} i^2 = k(k+1)(2k+1)/6 \qquad \text{(*)}$$

then

$$\sum_{i=1}^{k+1} i^2 = (k+1)((k+1)+1)(2(k+1)+1)/6 \qquad \text{(**)}$$

  - (e) *Proof of Induction Step*
  - Let k be any natural number.
  - Assume (Induction Hypothesis)

$$\sum_{i=1}^{k} i^2 = k(k+1)(2k+1)/6$$

$*$ We need to show (**) .

$$
\begin{aligned}
& LHS \\
= \; & \sum_{i=1}^{k+1} i^2 \\
= \; & (k+1)^2 + \sum_{i=1}^{k} i^2 \quad \text{Split off last term} \\
= \; & (k+1)^2 + k(k+1)(2k+1)/6 \quad \text{By the ind. hyp. (*)} \\
= \; & k^2 + 2k + 1 + \frac{(k^2+k)(2k+1)}{6} \quad \text{Expand} \\
= \; & k^2 + 2k + 1 + \frac{2k^3+3k^2+k}{6} \quad \text{Expand} \\
= \; & \frac{2k^3+9k^2+13k+6}{6} \quad \text{Put over common denom.}
\end{aligned}
$$

*

$$
\begin{aligned}
& RHS \\
= \; & \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6} \\
= \; & \frac{(k+1)(k+2)(2k+3)}{6} \text{ Adding} \\
= \; & \frac{(k^2+3k+2)(2k+3)}{6} \text{Expand} \\
= \; & \frac{2k^3+9k^2+13k+6}{6} \text{ Expand}
\end{aligned}
$$

* Thus we have (**)

- By the theorem of mathematical induction we have $\forall n \in \mathbb{N}, P(n)$.I.e. for all natural n,

$$\sum_{i=1}^{n} i^2 = n(n+1)(2n+1)/6$$

□

Example 2 If $|S| \in \mathbb{N}$ then $|\mathcal{P}(S)| = 2^{|S|}$.

Recall that $\mathcal{P}(S)$ is the set of all subsets of S

Proof:

- (a) Let $P(n)$ (for $n \in \mathbb{N}$) mean: for all sets S, if $|S| = n$ then $|\mathcal{P}(S)| = 2^n$
- We must show $\forall n \in \mathbb{N}$, for all sets S, if $|S| = n$ then $|\mathcal{P}(S)| = 2^n$
- (b) *Base Step:* We must show that all sets of cardinality 0 have a power set of size 2^0.
- (c) *Proof of Base step:*
  - ∗ There is only one set of size 0 namely $\emptyset$. The power set of $\emptyset$ is $\{\emptyset\}$ and has size 1, which equals 2^0
- (d) *Induction Step:* We must show that, for all $k \in \mathbb{N}$, if all sets of size k have a power set of size 2^k, then all sets of size $k+1$ have a power set of size 2^{k+1}.
- (e) *Proof of induction step:*
  - ∗ Let k be any natural number.
  - ∗ Assume (as Induction Hypothesis) that all sets of size k have a power set of size 2^k.

- ∗ Remains to prove: All sets of size $k+1$ have power sets of size 2^{k+1}
- ∗ Let S be any set of size $k+1$.
- ∗ Let x be any member of S.
- ∗ We can partition $\mathcal{P}(S)$ into two disjoint sets $Q = \{T \subseteq S \mid x \notin T\}$ and $R = \{T \subseteq S \mid x \in T\}$.
- ∗ Note. $\mathcal{P}(S) = Q \cup R$ and $Q \cap R = \emptyset$ So $|\mathcal{P}(S)| = |Q| + |R|$.
- ∗ Also note that each element of R can be obtained from an element of Q by "unioning in" x.
- ∗ And each element of Q can be obtained from an element of R by "subtracting out" x.
- ∗ So $|Q| = |R|$.
- ∗ Finally note that $Q = \mathcal{P}(S - \{x\})$ and since $|S - \{x\}| = k$ we have (by the ind. hyp.) $|Q| = 2^k$
- ∗ $|\mathcal{P}(S)| = |Q| + |R| = |Q| + |Q| = 2 \times 2^k = 2^{k+1}$

• By the theorem of mathematical induction
  $\forall n \in \mathbb{N},$ for all sets S, if $|S| = n$ then $|\mathcal{P}(S)| = 2^n$
  $\square$

Example of the construction of Q and R

$S = \{a, b, c, d\}$

If $x = a$ then we have

Q	R
$\{\emptyset$	$\{\{a\},$
$\{b\},$	$\{a, b\},$
$\{c\},$	$\{a, c\},$
$\{d\},$	$\{a, d\},$
$\{b, c\},$	$\{a, b, c\},$
$\{b, d\},$	$\{a, b, d\},$
$\{c, d\},$	$\{a, c, d\},$
$\{b, c, d\}\}$	$\{a, b, c, d\}\}$

Extending the principle

What if $P(0)$ isn't true? Or isn't meaningful. We can start from $P(1)$ or $P(2)$ and so on; even from $P(-42)$.

Principle: The theorem of (simple) mathematical induction (extended version).

- For any property P of the integers and $n_0 \in \mathbb{Z}$
  - $*$ if $P(n_0)$ and
  - $*$ for all $k \in \{n_0, n_0 + 1, ...\}$, if $P(k)$ then $P(k + 1)$
  - $*$ then $\forall n \in \{n_0, n_0 + 1, ...\}, P(n)$

Example 3: Call a set of straight lines in a plane "independent" if any two lines meet at a point and no three lines meet at a point.

Theorem. For $n \in \{1, 2, ...\}$ any set of n independent lines divides the plane into $\frac{n^2+n+2}{2}$

Proof

- So, by the theorem of simple mathematical induction (extended version) we have proved the theorem. □

Complete Induction

We can use a stronger induction hypothesis.

This often make the proof much easier.

Principle The theorem of complete mathematical induction:

The induction hypothesis here is:

- "for all integers j, with $0 \leq j < k$, $P(j)$" .

‘Informal Proof’:

$$\begin{array}{rl} & P(0) \wedge P(1) \wedge P(2) \wedge P(3) \wedge \cdots \\ \Leftrightarrow & P(0) \wedge \ (P(0) \to P(1)) \\ & \qquad \wedge \ (P(0) \wedge P(1) \to P(2)) \\ & \qquad \wedge \ (P(0) \wedge P(1) \wedge P(2) \to P(3)) \\ & \qquad \wedge \ \cdots \end{array}$$

Example 4

Consider the family of sequences defined by

$$\begin{array}{rcl} p_{a,0} & \triangleq & 1 \\ p_{a,n} & \triangleq & a \times p_{a,n-1} \text{ if } n > 0 \text{ and } n \text{ is odd} \\ p_{a,n} & \triangleq & \left(p_{a,n/2}\right)^2 \text{ if } n > 0 \text{ and } n \text{ is even} \end{array}$$

(For each value for a we get a sequence $p_{a,0}$, $p_{a,1}$, ...)

Make a table or two:

$a = 2$:

n	$p_{2,n}$
0	1
1	2
2	4
3	8
4	16

$a = 3$:

n	$p_{3,n}$
0	1
1	3
2	9
3	27
4	81

Theorem: for all $n \in \mathbb{N}$, $a \in \mathbb{R}$, we have $p_{a,n} = a^n$.

Note: For the purpose of this theorem we will consider $0^0 = 1$.

Proof by complete induction.

- Let $Q(n)$ mean that "for all $a \in \mathbb{R}$, we have $p_{a,n} = a^n$"
- Base step: We must show that $Q(0)$. I.e. that for all $a \in \mathbb{R}$, we have $p_{a,0} = a^0$"
- Proof of base step:
  - Let a be any real number.
  - $RHS = p_{a,0} = 1$, by defn of p
  - $LHS = a^0 = 1$
- Induction step: We must show that, for all $k \geq 1$, if $Q(j)$, for all $j \in \{0, 1, .., k-1\}$, then $Q(k)$.

  I.e. for all $k \geq 1$, if
  $$\forall j \in \{0, 1, .., k-1\}, \forall a \in \mathbb{R}, p_{a,j} = a^j \quad \text{(*)}$$
  then
  $$\forall a \in \mathbb{R}, p_{a,k} = a^k. \quad \text{(**)}$$
- Proof of induction step
  - Let k be any natural ≥ 1.

* Assume (as induction hypothesis) that

$$\forall j \in \{0, 1, .., k-1\}, \forall a \in \mathbb{R}, p_{a,j} = a^j$$

* Remains to show $\forall a \in \mathbb{R}, p_{a,k} = a^k$.
* Let a be any real number.
* Case that k is odd:
  · Then we know $p_{a,k} = a \times p_{a,k-1}$
  · Note that $0 \leq k-1 < k$.
  · We have

$$\begin{aligned} & p_{a,k} \\ = \ & a \times p_{a,k-1} && \text{Defn of } p \\ = \ & a \times a^{k-1} && \text{Ind. Hyp.} \\ = \ & a^k \end{aligned}$$

* Case that k is even:
  · Then by definition $p_{a,k} = \left(p_{a,k/2}\right)^2$
  · Note that $k/2$ is an integer and $0 \leq k/2 < k$.

· We have

$$
\begin{aligned}
& p_{a,k} \\
= \;& \left(p_{a,k/2}\right)^2 \quad \text{Defn of } p \\
= \;& \left(a^{k/2}\right)^2 \quad \text{Ind. Hyp.} \\
= \;& a^k
\end{aligned}
$$

- So, by the theorem of complete mathematical induction, we have the theorem. □

By the way, this leads to an efficient algorithm for computing exponents

---

```
double pow( double a, int p ) {
        if( p == 0 )
              return 1 ;
        else if( p & 1 )
              return a * pow( a, p-1 ) ;
        else {
              double b = pow( a, p/2 ) ;
              return b*b ; }
}
```

Extending Complete Induction

We can be a bit more general than this, allowing the base case to start anywhere and for multiple base cases.

Principle The theorem of complete induction (extended version)

- For any n_0 and n_1 in $\mathbb{Z}$ with $n_0 \leq n_1$ and property P of the integers
- If
  - [Base steps] $P(n_0)$ and $P(n_0 + 1)$ and ... and $P(n_1 - 1)$ and
  - [Induction step] for all integers $k \geq n_1$
    - if for all integers j, with $n_0 \leq j < k$, $P(j)$
    - then $P(k)$
- then, for all $n \in \{n_0, n_0 + 1, ...\}$, $P(n)$.

Here there are $n_1 - n_0$ base steps. Note that there can even be 0 base steps.

'Informal Proof' for $n_0 = 0$ and $n_1 = 2$

$$\begin{aligned} & P(0) \wedge P(1) \wedge P(2) \wedge P(3) \wedge \cdots \\ \Leftrightarrow\ & P(0) \wedge P(1) \wedge\ (P(0) \wedge P(1) \to P(2)) \\ & \qquad \wedge\ (P(0) \wedge P(1) \wedge P(2) \to P(3)) \wedge \cdots \end{aligned}$$

Example 5

Define the following "Fibonacci" sequence

$$\begin{aligned} fib_0 &\triangleq 1 \\ fib_1 &\triangleq 1 \\ fib_n &\triangleq fib_{n-1} + fib_{n-2}, \text{ if } n > 1 \end{aligned}$$

The Fibonacci sequence is $\langle 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \cdots \rangle$

Theorem: For all natural numbers n, $fib_n = ca^n + db^n$ where

$$c = \frac{5 + \sqrt{5}}{10} \qquad d = \frac{5 - \sqrt{5}}{10}$$

and

$$a = \frac{1 + \sqrt{5}}{2} \simeq 1.61803 \qquad b = \frac{1 - \sqrt{5}}{2} \simeq -0.61803$$

Note. At the moment this theorem appears from "thin air". Later in the course, we will develop a method for deriving this and similar theorems.

Note.

- The numbers a and b are the two solutions to the equation
$$\frac{1}{x} = x - 1$$
as you can see by the quadratic formula.
- The number a is often written ϕ and is called the "golden ratio".
- One consequence of the theorem is
$$\lim_{n\to\infty} \frac{fib_{n+1}}{fib_n} = \phi$$

Lemma: $\frac{1}{a} + \frac{1}{a^2} = 1 = \frac{1}{b} + \frac{1}{b^2}$

Proof of lemma:

$$\frac{1}{a} + \frac{1}{a^2} = \frac{1}{a} + \frac{1}{a}(a-1) = (a-1+1)\frac{1}{a} = a\frac{1}{a} = 1$$

And similarly for b. $\square$

Remark: Why this lemma? In actuality, I was most of the way through the proof of the theorem before I realized that this lemma would be useful. For presentation reasons it is convenient to prove it first.

Proof of theorem: By complete induction with 2 base cases.

The property $P(n)$ is "$fib_n = ca^n + db^n$"

First base step: for $n = 0$. We must show $fib_0 = ca^0 + db^0$

Proof of first base step

$$
\begin{aligned}
& ca^0 + db^0 \\
= \; & c + d \\
= \; & \frac{\left(5+\sqrt{5}\right)+\left(5-\sqrt{5}\right)}{10} \\
= \; & \frac{10}{10} \\
= \; & 1 \\
= \; & fib_0 \text{ by defn}
\end{aligned}
$$

Second base step: for $n = 1$. We must show $fib_1 = ca^1 + db^1$

Proof of second base step

$$
\begin{aligned}
& ca^1 + db^1 \\
= \; & \frac{5+\sqrt{5}}{10}\cdot\frac{1+\sqrt{5}}{2}+\frac{5-\sqrt{5}}{10}\cdot\frac{1-\sqrt{5}}{2} \\
= \; & \frac{\left(5+\sqrt{5}\right)\left(1+\sqrt{5}\right)+\left(5-\sqrt{5}\right)\left(1-\sqrt{5}\right)}{20} \\
= \; & \frac{5+6\sqrt{5}+5+5-6\sqrt{5}+5}{20} \\
= \; & 20/20 \\
= \; & 1
\end{aligned}
$$

Inductive step: We must show that for all integers $k \geq 2$, if, for all integers j, with $0 \leq j < k$, $P(j)$, then $P(k)$.

- Let k be any integer ≥ 2.
- Assume (as the ind. hyp.) that

for all j with $0 \leq j < k$, $fib_j = ca^j + db^j$ (*)

- In particular (as $k \geq 2$) the ind. hyp. implies that

$$fib_{k-1} = ca^{k-1} + db^{k-1} \quad (*1)$$

and that

$$fib_{k-2} = ca^{k-2} + db^{k-2} \quad (*2)$$

- It remains to show that $fib_k = ca^k + db^k$

$$\begin{aligned}
fib_k &= fib_{k-1} + fib_{k-2} && \text{Defn of } fib \text{ as } k \geq 2 \\
&= ca^{k-1} + db^{k-1} + ca^{k-2} + db^{k-2} && \text{From (*1) and (*2)} \\
&= c\left(a^{k-1} + a^{k-2}\right) + d\left(a^{k-1} + b^{k-2}\right) && \text{Distributivity} \\
&= c\left(\frac{a^k}{a} + \frac{a^k}{a^2}\right) + d\left(\frac{b^k}{b} + \frac{b^k}{b^2}\right) \\
&= ca^k\left(\frac{1}{a} + \frac{1}{a^2}\right) + db^k\left(\frac{1}{b} + \frac{1}{b^2}\right) && \text{Distributivity} \\
&= ca^k + db^k && \text{Lemma.}
\end{aligned}$$

So, by the theorem of complete mathematical induction, we have proved the theorem. □