The structure of natural numbers

is helpful for proving properties
$\forall n[n \in \mathbb{N} : P(n)]$

The structure of natural numbers

On natural numbers we can define a notion of a successor, a mapping

s: $\mathbb{N} \to \mathbb{N}$

by $s(n) = n+1$

The successor mapping imposes a structure on the set that enables us to count:

1) there is a starting natural number 0
2) for every natural number n, there is a next natural number $s(n) = n+1$.

(Some) Peano Axioms

Important properties

(1) Different natural numbers have different successors:

$\forall n,m\ [n,m \in \mathbb{N} : s(m) = s(n) \Rightarrow m = n]$

stated positively

s is injective!

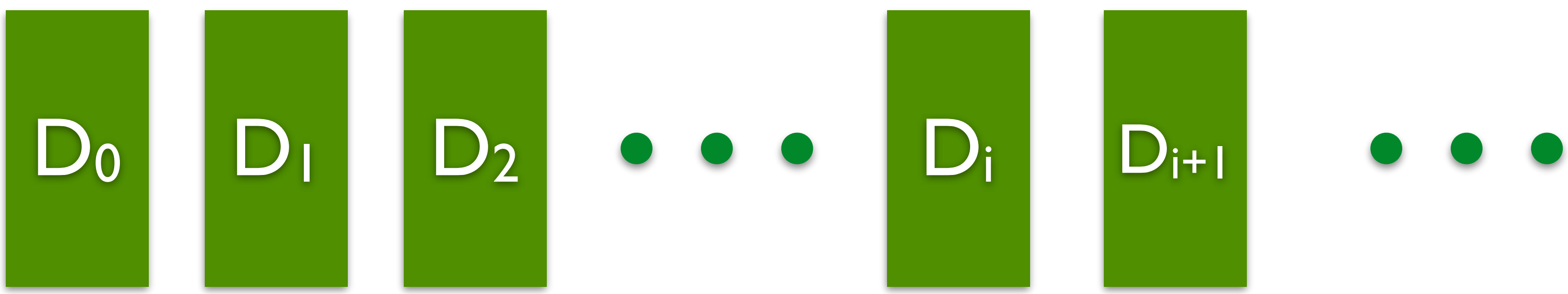
(2) 0 is not a successor: $\forall n\ [n \in \mathbb{N} : \neg\ (s(n) = 0)\ ]$

(3) All natural numbers except 0 are successors:

$\forall n[n \in \mathbb{N} \wedge \neg(n = 0) : \exists m[m \in \mathbb{N} : n = s(m)]$

There is more to it - induction

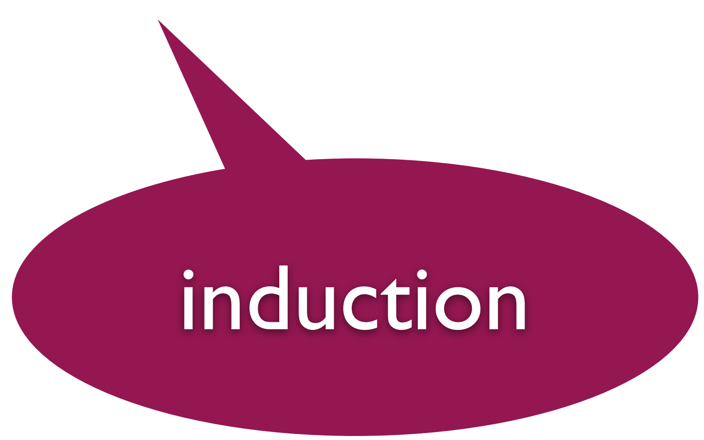
Imagine an infinite sequence of dominos



If we know that

1. D_0 falls
2. The dominos are close enough together so that if D_i falls, then D_{i+1} falls (for all $i \in \mathbb{N}$)

Then we can conclude that every domino D_n ($n \in \mathbb{N}$) falls!



Induction

P - unary predicate over $\mathbb{N}$

$P(0) \wedge \forall i\, [i \in \mathbb{N} : P(i) \Rightarrow P(i+1)] \Rightarrow \forall n\, [n \in \mathbb{N} : P(n)]$

$\forall$ elim with 0

$\Rightarrow$ elim

$\vdots$

$P(0)$
$P(0) \Rightarrow P(1)$
$P(1)$
$P(1) \Rightarrow P(2)$
$P(2)$
$P(2) \Rightarrow P(3)$
$\ldots$

Variant of the Peano Axiom:

Let $K \subseteq \mathbb{N}$ have the property that

(a) $0 \in K$ and

(b) for all $n \in \mathbb{N}$, $n \in K \Rightarrow (n+1) \in K$.

Then $K = \mathbb{N}$.

Induction

$P(0) \wedge \forall i\,[i \in \mathbb{N} : P(i) \Rightarrow P(i+1)] \;\Rightarrow \forall n\,[n \in \mathbb{N} : P(n)]$

P - unary predicate over $\mathbb{N}$

...

(m) $P(0)$

{Assume}

(k) $\boxed{\textbf{var } i;\, i \in \mathbb{N}}$

(k+1) $\boxed{P(i)}$

...

(l-1) $P(i+1)$

{$\Rightarrow$-intro on (k+1) and (l-1)}

(l) $P(i) \Rightarrow P(i+1)$

{$\forall$-intro on (k) and (l)}

(l+1) $\forall i[i \in \mathbb{N} : P(i) \Rightarrow P(i+1)]$

{induction on (m) and (l+1)}

(l+2) $\forall n[n \in \mathbb{N} : P(n)]$

Basis

induction hypothesis

Induction step

Inductive definitions

Inductive proof: truth is passed on

Inductive definition: construction is passed on

well defined by induction

Example

The sequence of real numbers $(a_i \mid i \in \mathbb{N})$ is defined inductively by

$$a_0 = 2$$
$$a_{i+1} = 2a_i - 1$$

a_0	a_1	a_2	a_3	a_4	…
2	3	5	9	17	…

proof by induction

Conjecture

For all $n \in \mathbb{N}$ it holds that

$$a_n = 2^n + 1$$

Strong induction

P - unary predicate over $\mathbb{N}$

$$\forall k\,[k \in \mathbb{N} : \forall j[j \in \mathbb{N} \wedge j < k : P(j)] \Rightarrow P(k)] \Rightarrow \forall n\,[n \in \mathbb{N} : P(n)]$$

$\forall$ elim with k=1

$\Rightarrow$ elim,

$\wedge$ intro

$P(0)$

$P(0) \Rightarrow P(1)$

$P(0) \wedge P(1)$

$P(0) \wedge P(1) \Rightarrow P(2)$

$P(0) \wedge P(1) \wedge P(2)$

$P(0) \wedge P(1) \wedge P(2) \Rightarrow P(3)$

...

Definition of $(a_i \mid i \in \mathbb{N})$ with strong induction

a_n is defined via $a_0, .., a_{n-1}$

Cardinality

Cardinals

Def. Two sets A and B have the same cardinality (are equinumerous) if there is a bijection $f: A \to B$.
Notation $A \sim B$, or $|A| = |B|$.

$|A| = [A]_{\sim}$

cardinal numbers are $\sim$ equivalence classes

Prop. The relation $\sim$ is an equivalence relation on sets.

Def. A set A has at most as large cardinality as a set B if there is an injection $f: A \to B$.
Notation $|A| \leq |B|$.

Def. A set A has at least as large cardinality as a set B if there is a surjection $f: A \to B$.
Notation $|A| \geq |B|$.

Def. A set A has smaller cardinality than a set B if there is an injection $f: A \to B$ and there is no surjection $f: A \to B$. Notation $|A| < |B|$.

Theorem (Cantor)

If $|A| \leq |B|$
and
$|B| \leq |A|$,
then
$|A| = |B|$.

Operations on cardinals

$|A| = [A]_{\sim}$

cardinal numbers are $\sim$ equivalence classes

Def. Let A and B be two disjoint sets. Then $|A| + |B| = |A \cup B|$.

Def. Let A and B be two sets. Then $|A| \cdot |B| = |A \times B|$.

Def. Let A and B be two sets. Then $|A|^{|B|} = |A^B|$ where A^B is the set of all functions from B to A, i.e. $A^B = \{f \mid f: B \to A\}$.

Prop. Let A be a set. Then $|\mathcal{P}(A)| = 2^{|A|}$.

Note: $2 = |\{0,1\}|$

Finite sets, finite cardinals

We write $\mathbb{N}_k$ for the set $\{0,1,..., k-1\}$. Then $\mathbb{N}_0 = \varnothing$.

We will also write k for $|\mathbb{N}_k|$.

$|A| = [A]_\sim$

Def. A set A is finite if and only if $|A| = k$, for some $k \in \mathbb{N}$.

cardinal numbers are ~ equivalence classes

Hence A set A is finite if and only if there is a natural number $k \in \mathbb{N}$ and a bijection $f: A \to \mathbb{N}_k$.

if and only if A has k elements, for some $k \in \mathbb{N}$

E.g. If $|A| = k$ and $|B| = m$ for some $k,m \in \mathbb{N}$

then $|A \times B| = k \cdot m$

The operations on cardinals when restricted to finite cardinals coincide with the operations on natural numbers!
This justifies the notation.

Infinite, countable and uncountable sets

Time for a video!

Hilbert's
infinite hotel :-)

Infinite, countable and uncountable sets

We write $\aleph_0$ for the cardinality of natural numbers.
Hence $\aleph_0 = |\mathbb{N}|$.

$|A| = [A]_\sim$

cardinal numbers are $\sim$ equivalence classes

Def. A set A is countable iff $|A| = \aleph_0$.

Prop.
$\mathbb{N}$ is countable.
$\mathbb{Z}$ is countable.
$\mathbb{Q}$ is countable.

Def. A set is infinite iff $|A| \geq \aleph_0$.

Hence, every countable set is infinite

Def. A set is uncountable iff $|A| > \aleph_0$.

Prop. $\mathbb{R}$ is uncountable.

We write c for $|\mathbb{R}|$

Cardinals are unbounded

$|A| = [A]_\sim$

cardinal numbers are ~ equivalence classes

Theorem (Cantor)

For every set A we have $|A| < |\mathcal{P}(A)|$.

Hence, for every cardinal there is a larger one.