Induction on the Natural Numbers

Assuming the Peano axioms and definition of Peano arithmetic found in "Defining Peano Arithmetic", and that shorthand for $\times\ (n, m)$ is nm.

Since the equality operation on natural numbers has been defined to be symmetric, it is okay to omit an implicit stage where you might say the initial statement is equal to the final statement when applying equalities.

Inductive Definitions of Functions

Addition, $+$, by induction on the left argument:

(1) $0 + y = y$
(2) $s(x) + y = s(x + y)$

Proof 1

Lemma 1: every natural number is even or odd, i.e. $\forall n.\ n \in \mathbb{N} \Rightarrow even(n) \vee odd(n)$

- $even(x) \coloneqq \exists m(m \in \mathbb{N} \Rightarrow x = 2m)$
- $odd(x) \coloneqq \exists m(m \in \mathbb{N} \Rightarrow x = 2m + 1)$
- Note that the successor of any even number is an odd number, and conversely the successor of any odd number is an even number.

Proof, by induction on n:

- Base case: show $0 \equiv 2(0)$, therefore 0 is even.
- IH: assume $even(k) \vee odd(k)$ for an arbitrary k.
- Step case: show that $even\big(s(k)\big) \vee odd\big(s(k)\big)$
  - If k is even:
    $s(k) \equiv s(2m)\ for\ some\ m \in \mathbb{N}$
    $s(2m) \equiv 2m + 1$
    $\therefore odd\big(s(k)\big)$
  - If k is odd:
    $s(k) \equiv s(2m + 1)\ for\ some\ m \in \mathbb{N}$
    $s(2m + 1) \equiv 2m + 1 + 1 \equiv 2m + 2 \equiv 2(m + 1)$
    $\therefore even\big(s(k)\big)$

Proof 2

Lemma 2: $\forall x. x \in \mathbb{N} \Rightarrow x + 0 = x$

Proof, by induction on x:

- Base case: show $0 + 0 = 0$, seen by (1).
- IH: assume $k + 0 = k$ for an arbitrary k.
- Step case: show that $s(k) + 0 = s(k)$
  $s(k) + 0 = s(k + 0)$ by (2)
  $= s(k)$ by IH

Proof 3

Lemma 3: addition is commutative, i.e. $\forall x, y \in \mathbb{N}.\ x + y = y + x$

Proof, by induction on x, i.e. $\forall x \in \mathbb{N}.\ \forall y \in \mathbb{N}(x + y = y + x)$:

- Base case: show $\forall y \in \mathbb{N}.\ 0 + y = y + 0$
  $0 + y = y$ by (1)
  $= y + 0$ by lemma 2
- IH: assume $\forall y \in \mathbb{N}.\ k + y = y + k$ for an arbitrary k.
- Step case: show that $\forall y \in \mathbb{N}.\ s(k) + y = y + s(k)$
  $s(k) + y = s(k + y)$ by (2)
  $= s(y + k)$ by IH
  $= s(y) + k$ by (2)
  notice there is nothing that can be done here further, requires lemma 4, which must be proved first
  $= y + s(k)$ by lemma 4

Proof 4

Lemma 4: $\forall x, y \in \mathbb{N}.\ s(x) + y = x + s(y)$

Proof, by induction on x, i.e. $\forall x \in \mathbb{N}.\ \forall y \in \mathbb{N}\big(s(x) + y = x + s(y)\big)$, ($x$ is good to choose as addition is defined by induction on the left argument):

- Base case: show $\forall y \in \mathbb{N}.\ s(0) + y = 0 + s(y)$
  $s(0) + y = s(0 + y)$ by (2)
  $= s(y)$ by (1)
  $= 0 + s(y)$ by (1)
- IH: assume $\forall y \in \mathbb{N}.\ s(k) + y = k + s(y)$ for an arbitrary k.
- Step case: show that $\forall y \in \mathbb{N}.\ s\big(s(k)\big) + y = s(k) + s(y)$
  $s\big(s(k)\big) + y = s(s(k) + y)$ by (2)
  $= s(k + s(y))$ by IH
  $= s(k) + s(y)$ by (2)

Induction on Lists

Given the inductive grammar for lists (the set ℓ) as $\ell ::= [\,] \mid x :: \ell$. And assuming the axioms and common laws of natural numbers and their operations (such as those previously shown), and the reflexivity, transitivity, and symmetry of equality on lists.

Recursive Definitions of Functions on Lists

Length, len, by induction on it's single argument:

(1) $len([\,]) = 0$
(2) $len(x :: xs) = 1 + len(xs)$

Append, @, by induction on the left argument:

(3) $[\,] \mathbin{@} ys = ys$
(4) $(x :: xs) \mathbin{@} ys = x :: (xs \mathbin{@} ys)$

Reverse, rev, by induction on it's single argument:

(5) $rev([\,]) = [\,]$
(6) $rev(x :: xs) = rev(xs) \mathbin{@} (x :: [\,])$

Proof 1

Lemma 1: $\forall xs, ys \in \ell.\ len(xs \mathbin{@} ys) = len(xs) + len(ys)$

Proof, by structural induction on xs (since @ is inductively defined on it's left argument):

- Base case: show $\forall ys \in \ell.\ len([\,] \mathbin{@} ys) = len([\,]) + len(ys)$
  $len([\,] \mathbin{@} ys) = len(ys)$ by (3)
  $= 0 + len(ys) = len([\,]) + len(ys)$ by (1)
- IH: assume $\forall ys \in \ell.\ len(ks \mathbin{@} ys) = len(ks) + len(ys)$ for an arbitrary list ks.
- Step case: show $\forall k.\ len\big((k :: ks) \mathbin{@} ys\big) = len(k :: ks) + len(ys)$
  $len\big((k :: ks) \mathbin{@} ys\big) = len\big(k :: (ks \mathbin{@} ys)\big)$ by (4)
  $= 1 + len(ks \mathbin{@} ys)$ by (2)
  $= 1 + len(ks) + len(ys)$ by IH
  $= len(k :: ks) + len(ys)$ by (2)

Proof 2

Lemma 2: $\forall xs \in \ell.\ len\big(rev(xs)\big) = len(xs)$

Proof, by structural induction on xs:

- Base case: show $len\big(rev([\,])\big) = len([\,])$
  $len\big(rev([\,])\big) = len([\,])$ by (5)
- IH: assume $len\big(rev(ks)\big) = len(ks)$ for an arbitrary list ks.
- Step case: show $\forall k.\ len\big(rev(k :: ks)\big) = len(k :: ks)$
  $len\big(rev(k :: ks)\big) = len\big(rev(ks) \mathbin{@} (k :: [\,])\big)$ by (6)
  $= len\big(rev(ks)\big) + len(k :: [\,])$ by lemma 1
  $= len(ks) + 1 + len([\,])$ by IH and (2)
  $= len(k :: ks) + 0$ by (2) and (1)
  $= len(k :: ks)$ by def. (+)

Induction on Binary Trees

Given the inductive grammar for binary trees (the set T) as $t ::= Lf \mid Br(x, t, t)$. And assuming the axioms and common laws of natural numbers and their operations (such as those previously shown), and the reflexivity, transitivity, and symmetry of equality on binary trees.

Recursive Definitions of Functions on Binary Trees

Size, $size$:

(1) $size(Lf) = 0$
(2) $size\big(Br(x, t_1, t_2)\big) = 1 + size(t_1) + size(t_2)$

Reflect, $refl$:

(3) $relf(Lf) = Lf$
(4) $refl\big(Br(x, t_1, t_2)\big) = Br\big(x, refl(t_2), refl(t_1)\big)$

Proof 1

Lemma 1: $\forall t \in T.\ refl\big(refl(t)\big) = t$

Proof, by structural induction on t:

- Base case: show $refl\big(refl(Lf)\big) = Lf$
  $refl\big(refl(Lf)\big) = refl(Lf) = Lf$ by (3) twice
- IH: assume $refl\big(refl(t_1)\big) = t_1$ and $refl\big(refl(t_2)\big) = t_2$ for arbitrary trees t_1 and t_2.
- Step case: show $\forall x.\ refl\Big(refl\big(Br(x, t_1, t_2)\big)\Big) = Br(x, t_1, t_2)$
  $refl\Big(refl\big(Br(x, t_1, t_2)\big)\Big) = refl\Big(Br\big(x, refl(t_2), refl(t_1)\big)\Big)$ by (4)
  $= Br\Big(x, refl\big(refl(t_1)\big), refl\big(refl(t_2)\big)\Big)$ by (4)
  $= Br(x, t_1, t_2)$ by IH

Proof 2

Lemma 2: $\forall t \in T.\ size\big(refl(t)\big) = size(t)$

Proof, by structural induction on t:

- Base case: show $size\big(refl(Lf)\big) = size(Lf)$
  $size\big(relf(Lf)\big) = size(Lf)$ by (3)
- IH: assume $size\big(refl(t_1)\big) = size(t_1)$ and $size\big(refl(t_2)\big) = size(t_2)$ for arbitrary trees t_1 and t_2.
- Step case: show $\forall x.\ size\Big(refl\big(Br(x, t_1, t_2)\big)\Big) = size\big(Br(x, t_1, t_2)\big)$
  $size\Big(refl\big(Br(x, t_1, t_2)\big)\Big) = size\Big(Br\big(x, refl(t_2), refl(t_1)\big)\Big)$ by (4)
  $= 1 + size\big(refl(t_2)\big) + size\big(refl(t_1)\big)$ by (2)
  $= 1 + size(t_2) + size(t_1)$ by IH
  $= 1 + size(t_1) + size(t_2)$ by commutativity of $(+)$
  $= size\big(Br(x, t_1, t_2)\big)$ by (2)

Induction on Propositional Formula

Given the inductive grammar for formulas (the set ϕ) as $\phi ::= A \mid \neg\phi \mid \phi \vee \phi$. And assuming the axioms and common laws of natural numbers and their operations (such as those previously shown), and the reflexivity, transitivity, and symmetry of equality on binary trees.

Proof 1

Lemma 1: every propositional formula φ has exactly one more occurrence of proposition letters than occurrences of ∨

Proof, by structural induction on φ:

- Base case: the proposition A

  Clearly there is 1 propositional letter A and no symbols (0 of) ∨, and $0 + 1 = 1$.
- IH 1: assume φ_1 has $n + 1$ occurrences of propositional letters, and n occurrences of ∨, where $n \in \mathbb{N}$.
- Step case 1: show that $\neg\varphi_1$ has $k + 1$ occurrences of propositional letters, and k occurrences of ∨, where $k \in \mathbb{N}$

  From IH 1, φ_1 has $n + 1$ and n occurrences of letters and ∨ respectively, and it is seen that $\neg\varphi$ does not add or remove occurrences of letters or ∨, hence $\neg\varphi_1$ has $n + 1$ and n occurrences of letters and ∨ respectively.
- IH 2: assume φ_1 has $n + 1$ occurrences of propositional letters and n occurrences of ∨, and that φ_2 has $m + 1$ occurrences of propositional letters and m occurrences of ∨, where $n, m \in \mathbb{N}$.
- Step case 2: show that $\varphi_1 \vee \varphi_2$ has $k + 1$ and k occurrences of letters and ∨ respectively, where $k \in \mathbb{N}$

  From IH 2, φ_1 has $n + 1$ and n letters and ∨ respectively, and φ_2 has $m + 1$ and m letters and ∨ respectively. $\varphi_1 \vee \varphi_2$ has all the occurrences in φ_1 and φ_2 and an additional occurrence of ∨.

  Proceeding to sum the occurrences of letters, $n + 1 + m + 1 = m + n + 1 + 1$, and summing the occurrences of ∨, $n + m + 1$, then clearly $k = n + m + 1$ and $k + 1 = k + 1$, hence there is one more occurrence of a letter in $\varphi_1 \vee \varphi_2$ than occurrences of ∨ in $\varphi_1 \vee \varphi_2$.

Two-Step Induction on the Natural Numbers

The same assumptions hold as previously for regular induction on the natural numbers.

Proof 1

Define the predicate $even$ inductively on $\mathbb{N}$ such that:

$$0 \in even$$
$$x \in \mathbb{N} \wedge x \in even \leftrightarrow s(s(x)) \in even$$
$$Nothing\ else\ is\ even.$$

I.e. the even numbers are $0, ss0, ssss0, ssssss0, \ldots$ (brackets are omitted for application of the successor function)

Lemma 1: $\forall x, y \in \mathbb{N}.\ even(x) \wedge even(y) \Rightarrow even(x + y)$

Proof by two-step induction on x:

- Base case 1: RTP $\forall y \in \mathbb{N}.\ even(0) \wedge even(y) \Rightarrow even(0 + y)$ valid
  $\equiv \top \wedge even(y) \Rightarrow even(y)$ by def. $(even)$ and def. $(+)$
  $\equiv even(y) \Rightarrow even(y)$ which is valid
- Base case 2: RTP $\forall y \in \mathbb{N}.\ even\big(s(0)\big) \wedge even(y) \Rightarrow even(s(0) + y)$ valid
  $\equiv \bot \wedge even(y) \Rightarrow even(s(0) + y)$ by def. $(even)$
  $\equiv \bot \Rightarrow even(s(0) + y)$ which is valid
- IH: assume $\forall y \in \mathbb{N}.\ even(k) \wedge even(y) \Rightarrow even(k + y)$ and $\forall y \in \mathbb{N}.\ even\big(s(k)\big) \wedge even(y) \Rightarrow even(s(k) + y)$ for an arbitrary $k, k \in \mathbb{N}$.
- Step case: show $\forall y \in \mathbb{N}.\ even\Big(s\big(s(k)\big)\Big) \wedge even(y) \Rightarrow even\big(s\big(s(k)\big) + y\big)$

  Assume: $even\Big(s\big(s(k)\big)\Big) \wedge even(y)$ is true. Show: $even\big(s\big(s(k)\big) + y\big)$ follows (is true in that case).

  By def. $(even)$, $even\Big(s\big(s(k)\big)\Big) \Rightarrow even(k)$

  By IH, $even(k + y)$

  $even\big(s\big(s(k)\big) + y\big) \equiv even\Big(s\big(s(k + y)\big)\Big)$ by earlier lemma

  $even(k + y) \Rightarrow even\Big(s\big(s(k + y)\big)\Big)$ by def. $(even)$

  Hence, $even(k + y) \Rightarrow even\big(s\big(s(k)\big) + y\big)$, so the consequent is valid whenever the IH is true.

Proofs by Infinite Descent on the Natural Numbers

Proof 1

Lemma 1: every natural number is even or odd, i.e. $\forall n \in \mathbb{N}. even(n) \vee odd(n)$

Recursive definition of predicate $even$:

$$even(0)$$

$$\forall n \in \mathbb{N}. even(n) \leftrightarrow even\Big(s\big(s(n)\big)\Big)$$

$$alternative\ def. \forall n \in \mathbb{N}. odd(n) \rightarrow even\big(s(n)\big)$$

Recursive definition of predicate odd:

$$odd(1)$$

$$\forall n \in \mathbb{N}. odd(n) \leftrightarrow odd\Big(s\big(s(n)\big)\Big)$$

$$alternative\ def. \forall n \in \mathbb{N}. even(n) \rightarrow odd\big(s(n)\big)$$

Proof, by infinite descent:

- Assume there is a counterexample $k, k \in \mathbb{N}$, i.e. $\neg\big(even(k) \vee odd(k)\big)$.
- Show that $\exists k' \in \mathbb{N}. k' < k \wedge \neg\big(even(k') \vee odd(k')\big)$:

- Clearly $k > 1$ as k is neither even nor odd (cannot be 0 or 1), so $k = s(s(k'))$ for $k' \in \mathbb{N}$.
- $\neg even(k) \rightarrow \neg even(k')$ by def. $(even)$
- $\neg odd(k) \rightarrow \neg odd(k')$ by def. (odd)
- Therefore, $\neg even(k) \wedge \neg odd(k) \rightarrow \neg even(k') \wedge \neg odd(k')$.

- Alternative from lecture slides:
  - Clearly $k > 0$, so $k = s(k')$.
  - $\neg even(k) \rightarrow \neg odd(k')$ and $\neg odd(k) \rightarrow \neg even(k')$, if $even$ and odd are defined with the alternative definitions for the recursive case, then the contrapositives give the result above, and hence $\neg even(k') \wedge \neg odd(k')$.
- There is therefore a $k' < k$ which is also a counterexample, which gives an infinite descent starting from k, which is a contradiction. Therefore, the initial assumption that there is a counterexample cannot be true, as it leads to a contradiction, so every natural number is even or odd.

Proof 2

Lemma 2: $\sqrt{2}$ is not rational, i.e. $\neg\exists x, y \in \mathbb{N}. \sqrt{2} = \frac{x}{y}$

Proof, by infinite descent:

- Assume that there exists counterexamples $a \in \mathbb{N}$ and $b \in \mathbb{N}$, i.e. $\sqrt{2} = \frac{a}{b}$.
- Show that there exists $c \in \mathbb{N}$ and $d \in \mathbb{N}$ where $\sqrt{2} = \frac{c}{d}$, where $c < a$ and $d < b$:

$$\sqrt{2} = \frac{a}{b} \Rightarrow 2b^2 = a^2 \Rightarrow a^2 - ab = 2b^2 - ab \Rightarrow a(a-b) = b(2b-a)$$
$$\Rightarrow \frac{2b-a}{a-b} = \frac{a}{b} = \sqrt{2}$$

  Let $a' = 2b - a$ and $b' = a - b$, $a', b' \in \mathbb{N}$.

  Notice $1 < \frac{a^2}{b^2} < 4$ (root 2 is between the roots of the next lowest and next highest perfect squares), so $1 < \frac{a}{b} < 2 \Rightarrow b < a < 2b$.

  Then $0 < a - b < b \Rightarrow 0 < b' < b$, and $b - a < 0 < 2b - a \Rightarrow 0 < a'$ and $2b - a < b < 3b - a \Rightarrow 2b - a < b < a \Rightarrow a' < a$.

  Which causes an infinite descent, which is a contradiction.
- As the initial assumption leads to a contradiction, $\sqrt{2}$ must be not be rational.

Proofs by Complete Induction on the Natural Numbers

Proof 1

Fundamental Theorem of Arithmetic (only the first part of the fundamental theorem): every natural number greater than or equal to 2 can be written as a product of prime numbers, i.e. $\forall n \in \mathbb{N}(2 \leq n \Rightarrow prime\ represenation\ of\ n)$

Proof, by complete induction on n:

- For an arbitrary $n \in \mathbb{N}$.
- Induction hypothesis: $\forall n' \in \mathbb{N}(n' < n \wedge 2 \leq n' \Rightarrow n'\ has\ a\ prime\ representation)$

- Step case: show n is a product of primes
    - Case 1: if n is prime, then it is clearly represented by itself.
    - Otherwise: $n = m \times k$, where $2 \leq m, k < n$. By IH m and k can be written as the product of prime numbers, therefore, so can $m \times k$.

This does require some definitions, such as being prime meaning a number is 1 multiplied by itself, and not prime meaning it is also, at least, the product of 2 numbers strictly smaller than itself.

Proof 2

Ackermann Function:

(1) $A(0, \mathrm{y}) = s(\mathrm{y})$
(2) $A(s(x), 0)) = A(x, 1)$
(3) $A\big(s(x), s(y)\big) = A\big(x, A(s(x), y)\big)$

Lexicographic Ordering:

$$(x', y') < (x, y) \equiv x' < x \vee (x' = x \wedge y' < y)$$

This provides a well-ordering for the set $\mathbb{N}^2$.

Lemma: $\forall x, y \in \mathbb{N}. A(x, y) \in \mathbb{N}$, i.e. $A(x, y)$ is defined.

Proof, by complete induction on (x, y):

- For an arbitrary (x, y), $x, y \in \mathbb{N}$.
- Induction hypothesis: assume $\forall x', y' \in \mathbb{N}. (x', y') < (x, y) \Rightarrow A(x', y') \in \mathbb{N}$.
- Step case: show $A(x, y) \in \mathbb{N}$, i.e. is defined
    - In the case where $x = 0$, $A(0, y) = s(y)$ which is clearly defined as the successor function s defined for all natural numbers.
    - In the case where $x \neq 0$, i.e. $x = s(a)$, $A(s(a), 0) = A(a, 1)$ by (2), which is defined by IH, since $(a, 1) < (x, 0)$.
    - In the case where $x, y \neq 0$, i.e. $x = s(a), y = s(b)$, then $A\big(s(a), s(b)\big) = A\big(a, A(s(a), b)\big)$ by (3), which is defined by IH, since $\big(a, A(s(a), b)\big) < (x, y)$.