MODULE *NaturalsInduction*

This module contains useful theorems for inductive proofs and recursive definitions over the naturals.

Some of the statements of the theorems are decomposed in terms of definitions. This is done for two reasons:

- It makes it easier for the backends to instantiate the theorems when those definitions are not expanded.
- It can be convenient when writing proofs to use those definitions rather than having to write out their expansions.

The proofs of these theorems appear in module *NaturalsInduction*_proofs.

EXTENDS $\mathit{Integers}$, TLAPS

The following is the simple statement of inductions over the naturals. For predicates P defined by a moderately complex operator, it is often useful to hide the operator definition before using this theorem. That is, you first define a suitable operator P (not necessarily by that name), prove the two hypotheses of the theorem, and then hide the definition of P when using the theorem.

THEOREM $\mathit{NatInduction} \triangleq$
  ASSUME NEW $P(\_)$,
    $P(0)$,
    $\forall n \in \mathit{Nat} : P(n) \Rightarrow P(n+1)$
  PROVE $\forall n \in \mathit{Nat} : P(n)$

A useful corollary of *NatInduction*

THEOREM $\mathit{DownwardNatInduction} \triangleq$
  ASSUME NEW $P(\_)$, NEW $m \in \mathit{Nat}$, $P(m)$,
    $\forall n \in 1 \,..\, m : P(n) \Rightarrow P(n-1)$
  PROVE $P(0)$

The following theorem expresses a stronger induction principle, also known as course-of-values induction, where the induction hypothesis is available for all strictly smaller natural numbers.

THEOREM $\mathit{GeneralNatInduction} \triangleq$
  ASSUME NEW $P(\_)$,
    $\forall n \in \mathit{Nat} : (\forall m \in 0 \,..\, (n-1) : P(m)) \Rightarrow P(n)$
  PROVE $\forall n \in \mathit{Nat} : P(n)$

The following theorem expresses the "least-number principle": if $P(n)$ is true for some natural number n then there is a smallest natural number for which P is true. It could be derived in module *WellFoundedInduction* as a corollary of the fact that the natural numbers are well ordered, but we give a direct proof.

THEOREM $\mathit{SmallestNatural} \triangleq$
  ASSUME NEW $P(\_)$, NEW $n \in \mathit{Nat}$, $P(n)$
  PROVE $\exists m \in \mathit{Nat} : \land P(m)$
    $\land \forall k \in 0 \,..\, m-1 : \neg P(k)$

The following theorem says that a recursively defined function f over the natural numbers is well-defined if for every $n \in \mathit{Nat}$ the definition of $f[n]$ depends only on arguments smaller than n.

THEOREM $\mathit{RecursiveFcnOfNat} \triangleq$
ASSUME NEW $\mathit{Def}(\_, \_)$,
ASSUME NEW $n \in \mathit{Nat}$, NEW g, NEW h,
$\forall\, i \in 0 \,..\, (n-1) : g[i] = h[i]$
PROVE $\mathit{Def}(g, n) = \mathit{Def}(h, n)$
PROVE LET $f[n \in \mathit{Nat}] \triangleq \mathit{Def}(f, n)$
IN $f = [n \in \mathit{Nat} \mapsto \mathit{Def}(f, n)]$

The following theorem *NatInductiveDef* is what you use to justify a function defined by primitive recursion over the naturals.

$\mathit{NatInductiveDefHypothesis}(f, f0, \mathit{Def}(\_, \_)) \triangleq$
$(f = $ CHOOSE $g : g = [i \in \mathit{Nat} \mapsto$ IF $i = 0$ THEN $f0$ ELSE $\mathit{Def}(g[i-1], i)])$
$\mathit{NatInductiveDefConclusion}(f, f0, \mathit{Def}(\_, \_)) \triangleq$
$f = [i \in \mathit{Nat} \mapsto$ IF $i = 0$ THEN $f0$ ELSE $\mathit{Def}(f[i-1], i)]$

THEOREM $\mathit{NatInductiveDef} \triangleq$
ASSUME NEW $\mathit{Def}(\_, \_)$, NEW f, NEW $f0$,
$\mathit{NatInductiveDefHypothesis}(f, f0, \mathit{Def})$
PROVE $\mathit{NatInductiveDefConclusion}(f, f0, \mathit{Def})$

The following two theorems allow you to prove the type of a recursively defined function over the natural numbers.

THEOREM $\mathit{RecursiveFcnOfNatType} \triangleq$
ASSUME NEW f, NEW S, NEW $\mathit{Def}(\_, \_)$, $f = [n \in \mathit{Nat} \mapsto \mathit{Def}(f, n)]$,
ASSUME NEW $n \in \mathit{Nat}$, NEW g, $\forall\, i \in 0 \,..\, n-1 : g[i] \in S$
PROVE $\mathit{Def}(g, n) \in S$
PROVE $f \in [\mathit{Nat} \rightarrow S]$

THEOREM $\mathit{NatInductiveDefType} \triangleq$
ASSUME NEW $\mathit{Def}(\_, \_)$, NEW S, NEW f, NEW $f0 \in S$,
$\mathit{NatInductiveDefConclusion}(f, f0, \mathit{Def})$,
$f0 \in S$,
$\forall\, v \in S, n \in \mathit{Nat} \setminus \{0\} : \mathit{Def}(v, n) \in S$
PROVE $f \in [\mathit{Nat} \rightarrow S]$

The following theorems show uniqueness of functions recursively defined over *Nat*.

THEOREM $\mathit{RecursiveFcnOfNatUnique} \triangleq$
ASSUME NEW $\mathit{Def}(\_, \_)$, NEW f, NEW g,
$f = [n \in \mathit{Nat} \mapsto \mathit{Def}(f, n)]$,
$g = [n \in \mathit{Nat} \mapsto \mathit{Def}(g, n)]$,
ASSUME NEW $n \in \mathit{Nat}$, NEW ff, NEW gg,
$\forall\, i \in 0 \,..\, (n-1) : \mathit{ff}[i] = \mathit{gg}[i]$
PROVE $\mathit{Def}(\mathit{ff}, n) = \mathit{Def}(\mathit{gg}, n)$
PROVE $f = g$

THEOREM $\mathit{NatInductiveUnique} \triangleq$
  ASSUME NEW $\mathit{Def}(\_, \_)$, NEW f, NEW g, NEW $f0$,
  $\mathit{NatInductiveDefConclusion}(f, f0, \mathit{Def})$,
  $\mathit{NatInductiveDefConclusion}(g, f0, \mathit{Def})$
  PROVE $f = g$

The following theorems are analogous to the preceding ones but for functions defined over intervals of natural numbers.

$\mathit{FiniteNatInductiveDefHypothesis}(f, c, \mathit{Def}(\_, \_), m, n) \triangleq$
  $(f =$ CHOOSE $g : g = [i \in m \,..\, n \mapsto$ IF $i = m$ THEN c ELSE $\mathit{Def}(g[i-1], i)])$
$\mathit{FiniteNatInductiveDefConclusion}(f, c, \mathit{Def}(\_, \_), m, n) \triangleq$
  $f = [i \in m \,..\, n \mapsto$ IF $i = m$ THEN c ELSE $\mathit{Def}(f[i-1], i)]$

THEOREM $\mathit{FiniteNatInductiveDef} \triangleq$
  ASSUME NEW $\mathit{Def}(\_, \_)$, NEW f, NEW c, NEW $m \in \mathit{Nat}$, NEW $n \in \mathit{Nat}$,
  $\mathit{FiniteNatInductiveDefHypothesis}(f, c, \mathit{Def}, m, n)$
  PROVE $\mathit{FiniteNatInductiveDefConclusion}(f, c, \mathit{Def}, m, n)$

THEOREM $\mathit{FiniteNatInductiveDefType} \triangleq$
  ASSUME NEW S, NEW $\mathit{Def}(\_, \_)$, NEW f, NEW $c \in S$, NEW $m \in \mathit{Nat}$, NEW $n \in \mathit{Nat}$,
  $\mathit{FiniteNatInductiveDefConclusion}(f, c, \mathit{Def}, m, n)$,
  $\forall v \in S, i \in (m+1) \,..\, n : \mathit{Def}(v, i) \in S$
  PROVE $f \in [m \,..\, n \rightarrow S]$

THEOREM $\mathit{FiniteNatInductiveUnique} \triangleq$
  ASSUME NEW $\mathit{Def}(\_, \_)$, NEW f, NEW g, NEW c, NEW $m \in \mathit{Nat}$, NEW $n \in \mathit{Nat}$,
  $\mathit{FiniteNatInductiveDefConclusion}(f, c, \mathit{Def}, m, n)$,
  $\mathit{FiniteNatInductiveDefConclusion}(g, c, \mathit{Def}, m, n)$
  PROVE $f = g$

(***)
(* The following theorems are analogous to the preceding ones but for *)
(* functions defined over intervals of natural numbers. *)
(***)

$\mathit{FiniteNatInductiveDefHypothesis}(f, c, \mathit{Def}(\_, \_), m, n) \triangleq$
  $(f =$ CHOOSE $g : g = [i \in m \,..\, n \mapsto$ IF $i = m$ THEN c ELSE $\mathit{Def}(g[i-1], i)])$
$\mathit{FiniteNatInductiveDefConclusion}(f, c, \mathit{Def}(\_, \_), m, n) \triangleq$
  $f = [i \in m \,..\, n \mapsto$ IF $i = m$ THEN c ELSE $\mathit{Def}(f[i-1], i)]$

THEOREM $\mathit{FiniteNatInductiveDef} \triangleq$
  ASSUME NEW $\mathit{Def}(\_, \_)$, NEW f, NEW c, NEW $m \in \mathit{Nat}$, NEW $n \in \mathit{Nat}$,
  $\mathit{FiniteNatInductiveDefHypothesis}(f, c, \mathit{Def}, m, n)$
  PROVE $\mathit{FiniteNatInductiveDefConclusion}(f, c, \mathit{Def}, m, n)$

THEOREM $\mathit{FiniteNatInductiveDefType} \triangleq$

ASSUME NEW S, NEW $Def(\_, \_)$, NEW f, NEW $c \in S$, NEW $m \in Nat$, NEW $n \in Nat$, $FiniteNatInductiveDefConclusion(f, c, Def, m, n)$, $\forall v \in S, i \in (m+1) \,..\, n : Def(v, i) \in S$
PROVE $f \in [m \,..\, n \to S]$

THEOREM $FiniteNatInductiveUnique \triangleq$
ASSUME NEW $Def(\_, \_)$, NEW f, NEW g, NEW c, NEW $m \in Nat$, NEW $n \in Nat$,
$FiniteNatInductiveDefConclusion(f, c, Def, m, n)$,
$FiniteNatInductiveDefConclusion(g, c, Def, m, n)$
PROVE $f = g$

(***
) (* The following example shows how this module is used. *)
(***)

$factorial[n \in Nat] \triangleq$ IF $n = 0$ THEN 1 ELSE $n * factorial[n-1]$

THEOREM $FactorialDefConclusion \triangleq NatInductiveDefConclusion(factorial, 1,$ LAMBDA $v, n : n * v)$
$\langle 1 \rangle 1.$ $NatInductiveDefHypothesis(factorial, 1,$ LAMBDA $v, n : n * v)$
BY DEF $NatInductiveDefHypothesis$, factorial
$\langle 1 \rangle 2.$ QED
BY $\langle 1 \rangle 1$, $NatInductiveDef$

THEOREM $FactorialDef \triangleq \forall n \in Nat : factorial[n] =$ IF $n = 0$ THEN 1 ELSE $n * factorial[n-1]$
BY $FactorialDefConclusion$ DEFS $NatInductiveDefConclusion$

THEOREM $FactorialType \triangleq$ factorial $\in [Nat \to Nat]$ $\langle 1 \rangle 1.$ $\forall v \in Nat, n \in Nat \setminus \{0\} : n * v \in Nat$
OBVIOUS
$\langle 1 \rangle 2.$ QED
BY $\langle 1 \rangle 1$, $1 \in Nat$, $NatInductiveDefType$, $FactorialDefConclusion$, Isa

---

\ * Modification History
\ * Last modified *Thu* May 08 12:29:46 *CEST* 2014 by *merz*
\ * Last modified *Tue Oct* 15 12:06:48 *CEST* 2013 by *shaolin*
\ * Last modified Sat *Nov* 26 08:49:59 *CET* 2011 by *merz*
\ * Last modified *Mon Nov* 07 08:58:05 *PST* 2011 by *lamport*
\ * Created *Mon Oct* 31 02:52:05 *PDT* 2011 by *lamport*