MODULE *Sets*

EXTENDS *Integers*, *NaturalsInduction*, *TLAPS*

    ∗ *NB*: Module *NaturalsInduction* comes from the *TLAPS* library, usually
    * installed in /usr/local/lib/tlaps. Make sure this is in your *Toolbox*
    * search path, see Preferences/TLA+ Preferences.

$$\mathit{IsBijection}(f, S, T) \triangleq \begin{array}{l} \land f \in [S \to T] \\ \land \forall x, y \in S : (x \neq y) \Rightarrow (f[x] \neq f[y]) \\ \land \forall y \in T : \exists x \in S : f[x] = y \end{array}$$

$$\mathit{IsFiniteSet}(S) \triangleq \exists n \in \mathit{Nat} : \exists f \; : \mathit{IsBijection}(f, 1 \mathrel{..} n, S)$$

Finite sets and cardinality are defined in the TLA+ standard module *FiniteSets*, but this is not yet natively supported by *TLAPS*. For the time being, we use the following axiom for defining set cardinality.

$\mathit{Cardinality}(S) \triangleq$ CHOOSE $n : (n \in \mathit{Nat}) \land \exists f : \mathit{IsBijection}(f, 1 \mathrel{..} n, S)$

CONSTANT $\mathit{Cardinality}(\_)$

AXIOM $\mathit{CardinalityAxiom} \triangleq$

$$\begin{array}{l} \forall S : \mathit{IsFiniteSet}(S) \Rightarrow \\ \quad \forall n : (n = \mathit{Cardinality}(S)) \equiv \\ \qquad\quad (n \in \mathit{Nat}) \land \exists f : \mathit{IsBijection}(f, 1 \mathrel{..} n, S) \end{array}$$

THEOREM $\mathit{CardinalityInNat} \triangleq \forall S : \mathit{IsFiniteSet}(S) \Rightarrow \mathit{Cardinality}(S) \in \mathit{Nat}$

BY *CardinalityAxiom*

THEOREM $\mathit{CardinalityZero} \triangleq$

$$\begin{array}{l} \land \mathit{IsFiniteSet}(\{\}) \\ \land \mathit{Cardinality}(\{\}) = 0 \\ \land \forall S : \mathit{IsFiniteSet}(S) \land (\mathit{Cardinality}(S) = 0) \Rightarrow (S = \{\}) \end{array}$$

$\langle 1\rangle 1.\ \land \mathit{IsFiniteSet}(\{\})$
        $\land \mathit{Cardinality}(\{\}) = 0$

  $\langle 2\rangle 1.\ \mathit{IsBijection}([x \in 1 \mathrel{..} 0 \mapsto \{\}], 1 \mathrel{..} 0, \{\})$
    BY *Z3* DEF *IsBijection*

  $\langle 2\rangle 2.$ QED
    BY $\langle 2\rangle 1$, *CardinalityAxiom* DEF *IsFiniteSet*

$\langle 1\rangle 2.$ ASSUME NEW S,
                $\mathit{IsFiniteSet}(S)$,
                $\mathit{Cardinality}(S) = 0$
        PROVE $S = \{\}$

  BY $\langle 1\rangle 2$, *CardinalityAxiom*, *SMT* DEF *IsBijection*

$\langle 1\rangle 3.$ QED
  BY $\langle 1\rangle 1$, $\langle 1\rangle 2$

```
THEOREM CardinalityPlusOne ≜
    ASSUME NEW S, IsFiniteSet(S),
           NEW x, x ∉ S
    PROVE  ∧ IsFiniteSet(S ∪ {x})
           ∧ Cardinality(S ∪ {x}) = Cardinality(S) + 1
⟨1⟩ DEFINE N ≜ Cardinality(S)
⟨1⟩1. PICK f : IsBijection(f, 1 .. N, S)
  BY CardinalityAxiom
⟨1⟩ DEFINE g ≜ [i ∈ 1 .. (N + 1) ↦ IF i = N + 1 THEN x ELSE f[i]]
⟨1⟩2. IsBijection(g, 1 .. (N + 1), S ∪ {x})
  BY ⟨1⟩1, CardinalityInNat, Z3 DEF IsBijection
⟨1⟩3. QED
  BY ⟨1⟩2, CardinalityInNat, CardinalityAxiom, SMT DEF IsFiniteSet

|------------------------------------------------------------------------|

THEOREM CardinalityOne ≜ ∀ m : ∧ IsFiniteSet({m})
                               ∧ Cardinality({m}) = 1
BY CardinalityZero, CardinalityPlusOne, IsaM("auto")

THEOREM CardinalityTwo ≜ ∀ m, p : m ≠ p ⇒
                              ∧ IsFiniteSet({m, p})
                              ∧ Cardinality({m, p}) = 2
BY CardinalityOne, CardinalityPlusOne, IsaM("auto")

THEOREM IntervalCardinality ≜
  ASSUME NEW a ∈ Nat, NEW b ∈ Nat
  PROVE  ∧ IsFiniteSet(a .. b)
         ∧ Cardinality(a .. b) = IF a > b THEN 0 ELSE b − a + 1
⟨1⟩1.CASE a > b
  BY ⟨1⟩1, CardinalityZero, a .. b = {}, IsFiniteSet(a .. b),
      Cardinality(a .. b) = 0, SMT
⟨1⟩2.CASE a ≤ b
  ⟨2⟩ DEFINE n ≜ b − a + 1
  ⟨2⟩ DEFINE F ≜ [x ∈ 1 .. n ↦ x + a − 1]
  ⟨2⟩1. ∀ y ∈ a .. b : ∃ x ∈ 1 .. n : y + 1 − a = x
     * This equation cannot be proved by SMTs if the variables are in a different order.
    BY ⟨1⟩2, SMT
  ⟨2⟩2. IsBijection(F, 1 .. n, a .. b)
    BY ⟨2⟩1, Z3 DEF IsBijection
  ⟨2⟩ QED
    BY ⟨2⟩2, ⟨1⟩2, CardinalityAxiom, SMT DEF IsFiniteSet
⟨1⟩q. QED
  BY ⟨1⟩1, ⟨1⟩2, SMT

|------------------------------------------------------------------------|
```

THEOREM $CardinalityOneConverse \triangleq$
    ASSUME NEW S, $IsFiniteSet(S)$, $Cardinality(S) = 1$
    PROVE $\exists\, m : S = \{m\}$
$\langle 1 \rangle 1.$ PICK $f : IsBijection(f,\ 1\,..\,1,\ S)$
  BY $CardinalityAxiom$
$\langle 1 \rangle 2.$ $S = \{f[1]\}$
  BY $\langle 1 \rangle 1$, SMT DEF $IsBijection$
$\langle 1 \rangle$q. QED
  BY $\langle 1 \rangle 2$

THEOREM $IsBijectionInverse \triangleq$
  ASSUME NEW f, NEW S, NEW T,
        $IsBijection(f,\ S,\ T)$
  PROVE $\exists\, g : IsBijection(g,\ T,\ S)$
$\langle 1 \rangle$ WITNESS $[y \in T \mapsto$ CHOOSE $x \in S : f[x] = y]$
$\langle 1 \rangle$ QED
  BY DEF $IsBijection$

THEOREM $IsBijectionTransitive \triangleq$
  ASSUME NEW $f1$, NEW $f2$, NEW S, NEW T, NEW U,
        $IsBijection(f1,\ S,\ U)$,
        $IsBijection(f2,\ U,\ T)$
  PROVE $\exists\, g : IsBijection(g,\ S,\ T)$
$\langle 1 \rangle$ WITNESS $[x \in S \mapsto f2[f1[x]]]$
$\langle 1 \rangle$ QED
  BY SMT DEF $IsBijection$

THEOREM
    ASSUME NEW $n \in Nat$, NEW $m \in Nat$,
        $IsBijection([x \in 1\,..\,n \mapsto x],\ 1\,..\,n,\ 1\,..\,m)$
    PROVE $n = m$

THEOREM $IsBijectionCardinality \triangleq$
  $\forall\, f,\ S,\ T :\ \land\ IsFiniteSet(S)$
        $\land\ IsFiniteSet(T)$
        $\Rightarrow (IsBijection(f,\ S,\ T) \equiv Cardinality(S) = Cardinality(T))$

LEMMA $CardinalitySetMinus \triangleq$
    ASSUME NEW S, $IsFiniteSet(S)$,
        NEW $x \in S$
    PROVE $\land\ IsFiniteSet(S \setminus \{x\})$
        $\land\ Cardinality(S \setminus \{x\}) = Cardinality(S) - 1$
$\langle 1 \rangle$ DEFINE $N \triangleq Cardinality(S)$
$\langle 1 \rangle 1.$ $IsFiniteSet(S \setminus \{x\})$
  $\langle 2 \rangle$g. PICK $g : IsBijection(g,\ 1\,..\,N,\ S)$

```
      BY CardinalityAxiom
    ⟨2⟩k. PICK k ∈ 1 .. N : g[k] = x
      BY ⟨2⟩g DEF IsBijection
    ⟨2⟩ ∧ N ∈ Nat
        ∧ N − 1 ∈ Nat
      BY CardinalityInNat, CardinalityZero, SMT
    ⟨2⟩ DEFINE f ≜ [i ∈ 1 .. N − 1 ↦ g[IF i < k THEN i ELSE i + 1]]
    ⟨2⟩ HIDE DEF f
    ⟨2⟩ SUFFICES IsBijection(f, 1 .. N − 1, S \ {x})
      BY DEF IsFiniteSet
    ⟨2⟩1. f ∈ [1 .. N − 1 → S \ {x}]
      BY ⟨2⟩g, ⟨2⟩k, SMT DEF IsBijection, f
    ⟨2⟩2. ASSUME NEW i ∈ 1 .. N − 1,
                 NEW j ∈ 1 .. N − 1,
                 i ≠ j
          PROVE  f[i] ≠ f[j]
      BY ⟨2⟩g, ⟨2⟩2, SMTT(30) DEF IsBijection, f
    ⟨2⟩3. ASSUME NEW y ∈ S \ {x}
          PROVE  ∃ i ∈ 1 .. N − 1 : f[i] = y
      ⟨3⟩j. PICK j ∈ 1 .. N : g[j] = y
        BY ⟨2⟩g DEF IsBijection
      ⟨3⟩1.CASE j < k
        BY ⟨3⟩j, ⟨3⟩1, Z3 DEF f
      ⟨3⟩2.CASE ¬(j < k)
        ⟨4⟩ ∧ ¬(j − 1 < k)
            ∧ (j − 1) + 1 = j
            ∧ j − 1 ∈ 1 .. N − 1
          BY ⟨3⟩j, ⟨3⟩2, ⟨2⟩k, SMT
        ⟨4⟩ QED
          BY ⟨3⟩j DEF f
      ⟨3⟩4. QED
        BY ⟨3⟩1, ⟨3⟩2
    ⟨2⟩q. QED
      BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3 DEF IsBijection
  ⟨1⟩2. Cardinality(S \ {x}) = Cardinality(S) − 1
    PROOF OMITTED
  ⟨1⟩q. QED
    BY ⟨1⟩1, ⟨1⟩2

THEOREM FiniteSubset ≜
  ASSUME NEW S, NEW TT, IsFiniteSet(TT), S ⊆ TT
  PROVE  ∧ IsFiniteSet(S)
         ∧ Cardinality(S) ≤ Cardinality(TT)
  ⟨1⟩2. PICK N ∈ Nat : N = Cardinality(TT)
    BY CardinalityAxiom
```

```
⟨1⟩3. IsFiniteSet(S)
  ⟨2⟩ DEFINE P(n) ≜ ∀ T : S ⊆ T ∧ IsFiniteSet(T) ∧ Cardinality(T) = n
                          ⇒ IsFiniteSet(S)
  ⟨2⟩2. P(0)
    BY CardinalityZero
  ⟨2⟩3. ASSUME NEW n ∈ Nat, P(n)
        PROVE  P(n + 1)
    ⟨3⟩1. SUFFICES ASSUME ∀ R : ∧ S ⊆ R
                                ∧ IsFiniteSet(R)
                                ∧ Cardinality(R) = n
                                ⇒ IsFiniteSet(S),
                          NEW T,
                          S ⊆ T,
                          IsFiniteSet(T),
                          Cardinality(T) = n + 1,
                          NEW x ∈ T, x ∉ S
                   PROVE  IsFiniteSet(S)
      BY ⟨2⟩3, SetExtensionality, SMT
    ⟨3⟩2. IsFiniteSet(T \ {x})
      BY ⟨3⟩1, CardinalitySetMinus
    ⟨3⟩q. QED
      BY ⟨3⟩1, ⟨3⟩2, CardinalityPlusOne, CardinalityInNat, SMT
  ⟨2⟩.HIDE DEF P
  ⟨2⟩4. ∀ n ∈ Nat : P(n)
    BY ⟨1⟩2, ⟨2⟩2, ⟨2⟩3, NatInduction
  ⟨2⟩q. QED
    BY ⟨1⟩2, ⟨2⟩4 DEF P
⟨1⟩4. Cardinality(S) ≤ Cardinality(TT)
  ⟨2⟩ DEFINE P(n) ≜ ∀ T : ∧ S ⊆ T
                          ∧ IsFiniteSet(T)
                          ∧ IsFiniteSet(S)
                          ∧ Cardinality(T) = n
                          ⇒ Cardinality(S) ≤ Cardinality(T)
  ⟨2⟩1. P(0)
    BY CardinalityZero, SetExtensionality, SMT
  ⟨2⟩2. ASSUME NEW n ∈ Nat, P(n)
        PROVE  P(n + 1)
    ⟨3⟩ SUFFICES ASSUME ∀ R :
                          ∧ S ⊆ R
                          ∧ IsFiniteSet(R)
                          ∧ IsFiniteSet(S)
                          ∧ Cardinality(R) = n
                          ⇒ Cardinality(S) ≤ Cardinality(R),
                        NEW T,
                        S ⊆ T,
```

```
                              IsFiniteSet(T),
                              IsFiniteSet(S),
                              Cardinality(T) = n + 1,
                              NEW x ∈ T, x ∉ S
                      PROVE Cardinality(S) ≤ Cardinality(T)
      BY ⟨2⟩2, SetExtensionality, SMT
    ⟨3⟩ ∧ IsFiniteSet(T \ {x})
        ∧ Cardinality(T \ {x}) = Cardinality(T) − 1
      BY CardinalitySetMinus
    ⟨3⟩ QED
      BY CardinalityPlusOne, CardinalityInNat, Z3
  ⟨2⟩ HIDE DEF P
  ⟨2⟩3. ∀ n ∈ Nat : P(n)
    BY ⟨1⟩2, ⟨2⟩1, ⟨2⟩2, NatInduction
  ⟨2⟩q. QED
    BY ⟨1⟩2, ⟨1⟩3, ⟨2⟩3, CardinalityInNat DEF P
⟨1⟩q. QED
  BY ⟨1⟩3, ⟨1⟩4
----------------------------------------------------------------------------

THEOREM CardinalityUnion ≜
            ∀ S, T : IsFiniteSet(S) ∧ IsFiniteSet(T) ⇒
                       ∧ IsFiniteSet(S ∪ T)
                       ∧ IsFiniteSet(S ∩ T)
                       ∧ Cardinality(S ∪ T) =
                             Cardinality(S) + Cardinality(T)
                             − Cardinality(S ∩ T)

----------------------------------------------------------------------------

THEOREM PigeonHole ≜
              ∀ S, T : ∧ IsFiniteSet(S)
                       ∧ IsFiniteSet(T)
                       ∧ Cardinality(T) < Cardinality(S)
                       ⇒ ∀ f ∈ [S → T] :
                            ∃ x, y ∈ S : x ≠ y ∧ f[x] = f[y]
⟨1⟩ DEFINE P(n) ≜ ∀ S : IsFiniteSet(S) ∧ (Cardinality(S) = n) ⇒
                     ∀ T : ∧ IsFiniteSet(T)
                           ∧ Cardinality(T) < Cardinality(S)
                           ⇒ ∀ f ∈ [S → T] :
                                ∃ x, y ∈ S : x ≠ y ∧ f[x] = f[y]

⟨1⟩2. SUFFICES ∀ n ∈ Nat : P(n)
  BY CardinalityInNat
⟨1⟩3. P(0)
  BY CardinalityInNat, SMT
```

```
⟨1⟩4. ASSUME NEW n ∈ Nat, P(n)
      PROVE   P(n + 1)
  ⟨2⟩ SUFFICES ASSUME NEW S, IsFiniteSet(S), Cardinality(S)  = n + 1,
                      NEW T, IsFiniteSet(T), Cardinality(T) < Cardinality(S),
                      NEW f ∈ [S → T]
               PROVE  ∃ x, y ∈ S : x ≠ y ∧ f[x] = f[y]
    OBVIOUS
  ⟨2⟩2. PICK z : z ∈ S
    ⟨3⟩1. S ≠ {}
      BY CardinalityZero, IsaM("force")
    ⟨3⟩2. QED
      BY ⟨3⟩1
  ⟨2⟩3.CASE ∃ w ∈ S : w ≠ z ∧ f[w] = f[z]
    BY ⟨2⟩2, ⟨2⟩3
  ⟨2⟩4.CASE ∀ w  ∈ S : w ≠ z ⇒ f[w] ≠ f[z]
    ⟨3⟩1. DEFINE g ≜ [w ∈ (S \ {z}) ↦ f[w]]
    ⟨3⟩2. ∃ x, y ∈ S \ {z} : x ≠ y ∧ g[x] = g[y]
      ⟨4⟩1. ∧ IsFiniteSet(S \ {z})
            ∧ Cardinality(S \ {z}) = (n + 1) − 1
            ∧ IsFiniteSet(T \ {f[z]})
            ∧ Cardinality(T \ {f[z]}) = Cardinality(T) − 1
        BY  ⟨2⟩1,⟨2⟩2, CardinalitySetMinus
      ⟨4⟩2. Cardinality(T \ {f[z]}) < Cardinality(S \ {z})
        BY  ⟨2⟩1,CardinalityInNat, ⟨4⟩1, SMT
      ⟨4⟩3. ∀ ff ∈ [S \ {z} → T \ {f[z]}] :
                 ∃ x, y ∈ S \ {z} : x ≠ y ∧ ff[x] = ff[y]
        BY ⟨1⟩4, ⟨4⟩1, ⟨4⟩2, IsaM("auto")
      ⟨4⟩4. g ∈ [S \ {z} → T \ {f[z]}]
        BY ⟨2⟩4
      ⟨4⟩ HIDE  DEF g
      ⟨4⟩5. QED
        BY ⟨4⟩4, ⟨4⟩3
    ⟨3⟩3.  QED
      BY ⟨3⟩2
  ⟨2⟩5. QED
    BY ⟨2⟩3, ⟨2⟩4
⟨1⟩ HIDE  DEF P
⟨1⟩5. QED
  BY ⟨1⟩3, ⟨1⟩4, NatInduction
├────────────────────────────────────────────────────────────────────┤

THEOREM ∀ S, T, f :  ∧ IsFiniteSet(S)
                     ∧ f ∈ [S → T]
                     ∧ ∀ y ∈ T : ∃ x ∈ S : y = f[x]
                     ⇒ ∧ IsFiniteSet(T)
```

$\land Cardinality(T) \leq Cardinality(S)$

PROOF OMITTED

THEOREM $ProductFinite \triangleq$

$\forall S,\ T : IsFiniteSet(S) \land IsFiniteSet(T) \Rightarrow IsFiniteSet(S \times T)$

PROOF OMITTED

THEOREM $SubsetsFinite \triangleq \forall S : IsFiniteSet(S) \Rightarrow IsFiniteSet(\text{SUBSET } S)$

PROOF OMITTED