

```

1 |----- MODULE Sets -----|
2 EXTENDS Integers, NaturalsInduction, TLAPS
3   * NB: Module NaturalsInduction comes from the TLAPS library, usually
4   * installed in /usr/local/lib/tlaps. Make sure this is in your Toolbox
5   * search path, see Preferences/TLA+ Preferences.

7 IsBijection(f, S, T)  $\triangleq$   $\wedge f \in [S \rightarrow T]$ 
8                                $\wedge \forall x, y \in S : (x \neq y) \Rightarrow (f[x] \neq f[y])$ 
9                                $\wedge \forall y \in T : \exists x \in S : f[x] = y$ 

12 IsFiniteSet(S)  $\triangleq \exists n \in \text{Nat} : \exists f : \text{IsBijection}(f, 1 \dots n, S)$ 

    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.

19 Cardinality(S)  $\triangleq$  CHOOSE n : (n  $\in$  Nat)  $\wedge \exists f : \text{IsBijection}(f, 1 \dots n, S)$ 

21 CONSTANT Cardinality(_)
22 AXIOM CardinalityAxiom  $\triangleq$ 
23      $\forall S : \text{IsFiniteSet}(S) \Rightarrow$ 
24      $\forall n : (n = \text{Cardinality}(S)) \equiv$ 
25      $(n \in \text{Nat}) \wedge \exists f : \text{IsBijection}(f, 1 \dots n, S)$ 
26 |-----|

28 THEOREM CardinalityInNat  $\triangleq \forall S : \text{IsFiniteSet}(S) \Rightarrow \text{Cardinality}(S) \in \text{Nat}$ 
29 BY CardinalityAxiom

31 |-----|

33 THEOREM CardinalityZero  $\triangleq$ 
34      $\wedge \text{IsFiniteSet}(\{\})$ 
35      $\wedge \text{Cardinality}(\{\}) = 0$ 
36      $\wedge \forall S : \text{IsFiniteSet}(S) \wedge (\text{Cardinality}(S) = 0) \Rightarrow (S = \{\})$ 
37  $\langle 1 \rangle 1. \wedge \text{IsFiniteSet}(\{\})$ 
38      $\wedge \text{Cardinality}(\{\}) = 0$ 
39  $\langle 2 \rangle 1. \text{IsBijection}([x \in 1 \dots 0 \mapsto \{\}], 1 \dots 0, \{\})$ 
40 BY Z3 DEF IsBijection
41  $\langle 2 \rangle 2. \text{QED}$ 
42 BY  $\langle 2 \rangle 1$ , CardinalityAxiom DEF IsFiniteSet
43  $\langle 1 \rangle 2. \text{ASSUME NEW } S,$ 
44     IsFiniteSet(S),
45     Cardinality(S) = 0
46 PROVE S = {}
47 BY  $\langle 1 \rangle 2$ , CardinalityAxiom, SMT DEF IsBijection
48  $\langle 1 \rangle 3. \text{QED}$ 
49 BY  $\langle 1 \rangle 1$ ,  $\langle 1 \rangle 2$ 

```

```

51 THEOREM CardinalityPlusOne  $\triangleq$ 
52   ASSUME NEW S, IsFiniteSet(S),
53     NEW x, x  $\notin$  S
54   PROVE  $\wedge$  IsFiniteSet(S  $\cup$  {x})
55      $\wedge$  Cardinality(S  $\cup$  {x}) = Cardinality(S) + 1
56 <1> DEFINE N  $\triangleq$  Cardinality(S)
57 <1>1. PICK f : IsBijection(f, 1 .. N, S)
58   BY CardinalityAxiom
59 <1> DEFINE g  $\triangleq$  [i  $\in$  1 .. (N + 1)  $\mapsto$  IF i = N + 1 THEN x ELSE f[i]]
60 <1>2. IsBijection(g, 1 .. (N + 1), S  $\cup$  {x})
61   BY <1>1, CardinalityInNat, Z3 DEF IsBijection
62 <1>3. QED
63   BY <1>2, CardinalityInNat, CardinalityAxiom, SMT DEF IsFiniteSet

```

```

67 THEOREM CardinalityOne  $\triangleq$   $\forall m : \wedge$  IsFiniteSet({m})
68    $\wedge$  Cardinality({m}) = 1
69 BY CardinalityZero, CardinalityPlusOne, IsaM("auto")

71 THEOREM CardinalityTwo  $\triangleq$   $\forall m, p : m \neq p \Rightarrow$ 
72    $\wedge$  IsFiniteSet({m, p})
73    $\wedge$  Cardinality({m, p}) = 2
74 BY CardinalityOne, CardinalityPlusOne, IsaM("auto")

```

```

76 THEOREM IntervalCardinality  $\triangleq$ 
77   ASSUME NEW a  $\in$  Nat, NEW b  $\in$  Nat
78   PROVE  $\wedge$  IsFiniteSet(a .. b)
79      $\wedge$  Cardinality(a .. b) = IF a > b THEN 0 ELSE b - a + 1
80 <1>1.CASE a > b
81   BY <1>1, CardinalityZero, a .. b = {}, IsFiniteSet(a .. b),
82     Cardinality(a .. b) = 0, SMT
83 <1>2.CASE a  $\leq$  b
84   <2> DEFINE n  $\triangleq$  b - a + 1
85   <2> DEFINE F  $\triangleq$  [x  $\in$  1 .. n  $\mapsto$  x + a - 1]
86   <2>1.  $\forall y \in a \dots b : \exists x \in 1 \dots n : y + 1 - a = x$ 

```

* This equation cannot be proved by *SMT*s if the variables are in a different order.

```

89   BY <1>2, SMT
90   <2>2. IsBijection(F, 1 .. n, a .. b)
91     BY <2>1, Z3 DEF IsBijection
92   <2> QED
93   BY <2>2, <1>2, CardinalityAxiom, SMT DEF IsFiniteSet
94 <1>q. QED
95   BY <1>1, <1>2, SMT

```

```

99 THEOREM CardinalityOneConverse  $\triangleq$ 
100   ASSUME NEW  $S$ , IsFiniteSet( $S$ ), Cardinality( $S$ ) = 1
101   PROVE  $\exists m : S = \{m\}$ 
102   <1>1. PICK  $f : \text{IsBijection}(f, 1 \dots 1, S)$ 
103   BY CardinalityAxiom
104   <1>2.  $S = \{f[1]\}$ 
105   BY <1>1, SMT DEF IsBijection
106   <1>q. QED
107   BY <1>2

```

```

111 THEOREM IsBijectionInverse  $\triangleq$ 
112   ASSUME NEW  $f$ , NEW  $S$ , NEW  $T$ ,
113           IsBijection( $f, S, T$ )
114   PROVE  $\exists g : \text{IsBijection}(g, T, S)$ 
115   <1> WITNESS [ $y \in T \mapsto \text{CHOOSE } x \in S : f[x] = y$ ]
116   <1> QED
117   BY DEF IsBijection

```

```

119 THEOREM IsBijectionTransitive  $\triangleq$ 
120   ASSUME NEW  $f1$ , NEW  $f2$ , NEW  $S$ , NEW  $T$ , NEW  $U$ ,
121           IsBijection( $f1, S, U$ ),
122           IsBijection( $f2, U, T$ )
123   PROVE  $\exists g : \text{IsBijection}(g, S, T)$ 
124   <1> WITNESS [ $x \in S \mapsto f2[f1[x]]$ ]
125   <1> QED
126   BY SMT DEF IsBijection

```

```

128 THEOREM
129   ASSUME NEW  $n \in \text{Nat}$ , NEW  $m \in \text{Nat}$ ,
130           IsBijection( $[x \in 1 \dots n \mapsto x], 1 \dots n, 1 \dots m$ )
131   PROVE  $n = m$ 

```

```

133 THEOREM IsBijectionCardinality  $\triangleq$ 
134    $\forall f, S, T : \wedge \text{IsFiniteSet}(S)$ 
135                $\wedge \text{IsFiniteSet}(T)$ 
136                $\Rightarrow (\text{IsBijection}(f, S, T) \equiv \text{Cardinality}(S) = \text{Cardinality}(T))$ 

```

```

138 LEMMA CardinalitySetMinus  $\triangleq$ 
139   ASSUME NEW  $S$ , IsFiniteSet( $S$ ),
140           NEW  $x \in S$ 
141   PROVE  $\wedge \text{IsFiniteSet}(S \setminus \{x\})$ 
142            $\wedge \text{Cardinality}(S \setminus \{x\}) = \text{Cardinality}(S) - 1$ 
143   <1> DEFINE  $N \triangleq \text{Cardinality}(S)$ 
144   <1>1. IsFiniteSet( $S \setminus \{x\}$ )
145   <2>g. PICK  $g : \text{IsBijection}(g, 1 \dots N, S)$ 

```

```

146     BY CardinalityAxiom
147   ⟨2⟩k. PICK  $k \in 1 \dots N : g[k] = x$ 
148     BY ⟨2⟩g DEF IsBijection
149   ⟨2⟩  $\wedge N \in \text{Nat}$ 
150      $\wedge N - 1 \in \text{Nat}$ 
151     BY CardinalityInNat, CardinalityZero, SMT
152   ⟨2⟩ DEFINE  $f \triangleq [i \in 1 \dots N - 1 \mapsto g[\text{IF } i < k \text{ THEN } i \text{ ELSE } i + 1]]$ 
153   ⟨2⟩ HIDE DEF  $f$ 
154   ⟨2⟩ SUFFICES IsBijection( $f, 1 \dots N - 1, S \setminus \{x\}$ )
155     BY DEF IsFiniteSet
156   ⟨2⟩1.  $f \in [1 \dots N - 1 \rightarrow S \setminus \{x\}]$ 
157     BY ⟨2⟩g, ⟨2⟩k, SMT DEF IsBijection,  $f$ 
158   ⟨2⟩2. ASSUME NEW  $i \in 1 \dots N - 1$ ,
159         NEW  $j \in 1 \dots N - 1$ ,
160          $i \neq j$ 
161         PROVE  $f[i] \neq f[j]$ 
162     BY ⟨2⟩g, ⟨2⟩2, SMTT(30) DEF IsBijection,  $f$ 
163   ⟨2⟩3. ASSUME NEW  $y \in S \setminus \{x\}$ 
164         PROVE  $\exists i \in 1 \dots N - 1 : f[i] = y$ 
165     ⟨3⟩j. PICK  $j \in 1 \dots N : g[j] = y$ 
166         BY ⟨2⟩g DEF IsBijection
167     ⟨3⟩1.CASE  $j < k$ 
168         BY ⟨3⟩j, ⟨3⟩1, Z3 DEF  $f$ 
169     ⟨3⟩2.CASE  $\neg(j < k)$ 
170         ⟨4⟩  $\wedge \neg(j - 1 < k)$ 
171              $\wedge (j - 1) + 1 = j$ 
172              $\wedge j - 1 \in 1 \dots N - 1$ 
173             BY ⟨3⟩j, ⟨3⟩2, ⟨2⟩k, SMT
174         ⟨4⟩ QED
175         BY ⟨3⟩j DEF  $f$ 
176     ⟨3⟩4. QED
177     BY ⟨3⟩1, ⟨3⟩2
178   ⟨2⟩q. QED
179     BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3 DEF IsBijection
180   ⟨1⟩2. Cardinality( $S \setminus \{x\}$ ) = Cardinality( $S$ ) - 1
181     PROOF OMITTED
182   ⟨1⟩q. QED
183     BY ⟨1⟩1, ⟨1⟩2

185 THEOREM FiniteSubset  $\triangleq$ 
186   ASSUME NEW  $S$ , NEW  $TT$ , IsFiniteSet( $TT$ ),  $S \subseteq TT$ 
187   PROVE  $\wedge \text{IsFiniteSet}(S)$ 
188          $\wedge \text{Cardinality}(S) \leq \text{Cardinality}(TT)$ 
189   ⟨1⟩2. PICK  $N \in \text{Nat} : N = \text{Cardinality}(TT)$ 
190     BY CardinalityAxiom

```

191 $\langle 1 \rangle 3. \text{ } IsFiniteSet(S)$
192 $\langle 2 \rangle \text{ DEFINE } P(n) \triangleq \forall T : S \subseteq T \wedge IsFiniteSet(T) \wedge Cardinality(T) = n$
193 $\Rightarrow IsFiniteSet(S)$
194 $\langle 2 \rangle 2. P(0)$
195 BY *CardinalityZero*
196 $\langle 2 \rangle 3. \text{ ASSUME NEW } n \in Nat, P(n)$
197 PROVE $P(n + 1)$
198 $\langle 3 \rangle 1. \text{ SUFFICES ASSUME } \forall R : \wedge S \subseteq R$
199 $\wedge IsFiniteSet(R)$
200 $\wedge Cardinality(R) = n$
201 $\Rightarrow IsFiniteSet(S),$
202 NEW $T,$
203 $S \subseteq T,$
204 $IsFiniteSet(T),$
205 $Cardinality(T) = n + 1,$
206 NEW $x \in T, x \notin S$
207 PROVE $IsFiniteSet(S)$
208 BY $\langle 2 \rangle 3, SetExtensionality, SMT$
209 $\langle 3 \rangle 2. IsFiniteSet(T \setminus \{x\})$
210 BY $\langle 3 \rangle 1, CardinalitySetMinus$
211 $\langle 3 \rangle q. \text{ QED}$
212 BY $\langle 3 \rangle 1, \langle 3 \rangle 2, CardinalityPlusOne, CardinalityInNat, SMT$
213 $\langle 2 \rangle \text{.HIDE DEF } P$
214 $\langle 2 \rangle 4. \forall n \in Nat : P(n)$
215 BY $\langle 1 \rangle 2, \langle 2 \rangle 2, \langle 2 \rangle 3, NatInduction$
216 $\langle 2 \rangle q. \text{ QED}$
217 BY $\langle 1 \rangle 2, \langle 2 \rangle 4 \text{ DEF } P$
218 $\langle 1 \rangle 4. Cardinality(S) \leq Cardinality(TT)$
219 $\langle 2 \rangle \text{ DEFINE } P(n) \triangleq \forall T : \wedge S \subseteq T$
220 $\wedge IsFiniteSet(T)$
221 $\wedge IsFiniteSet(S)$
222 $\wedge Cardinality(T) = n$
223 $\Rightarrow Cardinality(S) \leq Cardinality(T)$
224 $\langle 2 \rangle 1. P(0)$
225 BY *CardinalityZero, SetExtensionality, SMT*
226 $\langle 2 \rangle 2. \text{ ASSUME NEW } n \in Nat, P(n)$
227 PROVE $P(n + 1)$
228 $\langle 3 \rangle \text{ SUFFICES ASSUME } \forall R :$
229 $\wedge S \subseteq R$
230 $\wedge IsFiniteSet(R)$
231 $\wedge IsFiniteSet(S)$
232 $\wedge Cardinality(R) = n$
233 $\Rightarrow Cardinality(S) \leq Cardinality(R),$
234 NEW $T,$
235 $S \subseteq T,$

236 $IsFiniteSet(T),$
237 $IsFiniteSet(S),$
238 $Cardinality(T) = n + 1,$
239 $NEW\ x \in T, x \notin S$
240 $PROVE\ Cardinality(S) \leq Cardinality(T)$
241 $BY\ \langle 2 \rangle 2, SetExtensionality, SMT$
242 $\langle 3 \rangle \wedge IsFiniteSet(T \setminus \{x\})$
243 $\wedge Cardinality(T \setminus \{x\}) = Cardinality(T) - 1$
244 $BY\ CardinalitySetMinus$
245 $\langle 3 \rangle\ QED$
246 $BY\ CardinalityPlusOne, CardinalityInNat, Z3$
247 $\langle 2 \rangle\ HIDE\ DEF\ P$
248 $\langle 2 \rangle 3. \forall n \in Nat : P(n)$
249 $BY\ \langle 1 \rangle 2, \langle 2 \rangle 1, \langle 2 \rangle 2, NatInduction$
250 $\langle 2 \rangle q. QED$
251 $BY\ \langle 1 \rangle 2, \langle 1 \rangle 3, \langle 2 \rangle 3, CardinalityInNat\ DEF\ P$
252 $\langle 1 \rangle q. QED$
253 $BY\ \langle 1 \rangle 3, \langle 1 \rangle 4$
254 |-----|

256 $THEOREM\ CardinalityUnion \triangleq$
257 $\forall S, T : IsFiniteSet(S) \wedge IsFiniteSet(T) \Rightarrow$
258 $\wedge IsFiniteSet(S \cup T)$
259 $\wedge IsFiniteSet(S \cap T)$
260 $\wedge Cardinality(S \cup T) =$
261 $Cardinality(S) + Cardinality(T)$
262 $- Cardinality(S \cap T)$
264 |-----|

266 $THEOREM\ PigeonHole \triangleq$
267 $\forall S, T : \wedge IsFiniteSet(S)$
268 $\wedge IsFiniteSet(T)$
269 $\wedge Cardinality(T) < Cardinality(S)$
270 $\Rightarrow \forall f \in [S \rightarrow T] :$
271 $\exists x, y \in S : x \neq y \wedge f[x] = f[y]$
272 $\langle 1 \rangle\ DEFINE\ P(n) \triangleq \forall S : IsFiniteSet(S) \wedge (Cardinality(S) = n) \Rightarrow$
273 $\forall T : \wedge IsFiniteSet(T)$
274 $\wedge Cardinality(T) < Cardinality(S)$
275 $\Rightarrow \forall f \in [S \rightarrow T] :$
276 $\exists x, y \in S : x \neq y \wedge f[x] = f[y]$
278 $\langle 1 \rangle 2. SUFFICES\ \forall n \in Nat : P(n)$
279 $BY\ CardinalityInNat$
280 $\langle 1 \rangle 3. P(0)$
281 $BY\ CardinalityInNat, SMT$

282 $\langle 1 \rangle 4.$ ASSUME NEW $n \in \text{Nat}, P(n)$
 283 PROVE $P(n + 1)$
 284 $\langle 2 \rangle$ SUFFICES ASSUME NEW $S, \text{IsFiniteSet}(S), \text{Cardinality}(S) = n + 1,$
 285 NEW $T, \text{IsFiniteSet}(T), \text{Cardinality}(T) < \text{Cardinality}(S),$
 286 NEW $f \in [S \rightarrow T]$
 287 PROVE $\exists x, y \in S : x \neq y \wedge f[x] = f[y]$
 288 OBVIOUS
 289 $\langle 2 \rangle 2.$ PICK $z : z \in S$
 290 $\langle 3 \rangle 1.$ $S \neq \{\}$
 291 BY $\text{CardinalityZero}, \text{IsaM}(\text{"force"})$
 292 $\langle 3 \rangle 2.$ QED
 293 BY $\langle 3 \rangle 1$
 294 $\langle 2 \rangle 3.$ CASE $\exists w \in S : w \neq z \wedge f[w] = f[z]$
 295 BY $\langle 2 \rangle 2, \langle 2 \rangle 3$
 296 $\langle 2 \rangle 4.$ CASE $\forall w \in S : w \neq z \Rightarrow f[w] \neq f[z]$
 297 $\langle 3 \rangle 1.$ DEFINE $g \triangleq [w \in (S \setminus \{z\}) \mapsto f[w]]$
 298 $\langle 3 \rangle 2.$ $\exists x, y \in S \setminus \{z\} : x \neq y \wedge g[x] = g[y]$
 299 $\langle 4 \rangle 1.$ $\wedge \text{IsFiniteSet}(S \setminus \{z\})$
 300 $\wedge \text{Cardinality}(S \setminus \{z\}) = (n + 1) - 1$
 301 $\wedge \text{IsFiniteSet}(T \setminus \{f[z]\})$
 302 $\wedge \text{Cardinality}(T \setminus \{f[z]\}) = \text{Cardinality}(T) - 1$
 303 BY $\langle 2 \rangle 1, \langle 2 \rangle 2, \text{CardinalitySetMinus}$
 304 $\langle 4 \rangle 2.$ $\text{Cardinality}(T \setminus \{f[z]\}) < \text{Cardinality}(S \setminus \{z\})$
 305 BY $\langle 2 \rangle 1, \text{CardinalityInNat}, \langle 4 \rangle 1, \text{SMT}$
 306 $\langle 4 \rangle 3.$ $\forall ff \in [S \setminus \{z\} \rightarrow T \setminus \{f[z]\}] :$
 307 $\exists x, y \in S \setminus \{z\} : x \neq y \wedge ff[x] = ff[y]$
 308 BY $\langle 1 \rangle 4, \langle 4 \rangle 1, \langle 4 \rangle 2, \text{IsaM}(\text{"auto"})$
 309 $\langle 4 \rangle 4.$ $g \in [S \setminus \{z\} \rightarrow T \setminus \{f[z]\}]$
 310 BY $\langle 2 \rangle 4$
 311 $\langle 4 \rangle$ HIDE DEF g
 312 $\langle 4 \rangle 5.$ QED
 313 BY $\langle 4 \rangle 4, \langle 4 \rangle 3$
 314 $\langle 3 \rangle 3.$ QED
 315 BY $\langle 3 \rangle 2$
 316 $\langle 2 \rangle 5.$ QED
 317 BY $\langle 2 \rangle 3, \langle 2 \rangle 4$
 318 $\langle 1 \rangle$ HIDE DEF P
 319 $\langle 1 \rangle 5.$ QED
 320 BY $\langle 1 \rangle 3, \langle 1 \rangle 4, \text{NatInduction}$
 321

 323 THEOREM $\forall S, T, f : \wedge \text{IsFiniteSet}(S)$
 324 $\wedge f \in [S \rightarrow T]$
 325 $\wedge \forall y \in T : \exists x \in S : y = f[x]$
 326 $\Rightarrow \wedge \text{IsFiniteSet}(T)$

327 $\wedge \text{Cardinality}(T) \leq \text{Cardinality}(S)$

328 PROOF OMITTED

330 THEOREM $\text{ProductFinite} \stackrel{\Delta}{=}$

331 $\forall S, T : \text{IsFiniteSet}(S) \wedge \text{IsFiniteSet}(T) \Rightarrow \text{IsFiniteSet}(S \times T)$

332 PROOF OMITTED

334 THEOREM $\text{SubsetsFinite} \stackrel{\Delta}{=}$ $\forall S : \text{IsFiniteSet}(S) \Rightarrow \text{IsFiniteSet}(\text{SUBSET } S)$

335 PROOF OMITTED

336