Cyclic core computation specification and proofs

Ioannis Filippidis

December 22, 2017
URL update on July 23, 2018

Abstract

A TLA$^+$ specification and proofs of relevant properties for an algorithm that computes the cyclic core of a minimal covering problem. This algorithm was originally proposed in the context of two-level logic minimization. The modules *FiniteSetTheorems*, *Functions*, *FunctionTheorems*, *NaturalsInduction*, *SequenceTheorems*, *TLAPS*, *WellFoundedInduction* can be found in the distribution of TLAPS v1.4.3: `http://tla.msr-inria.inria.fr/tlaps/dist/current/tlaps-1.4.3.tar.gz`. This document accompanies the dissertation available at: `http://resolver.caltech.edu/CaltechTHESIS:07202018-115217471`.

Contents

MODULE *FiniteSetFacts*

Additions to the module *FiniteSetTheorems from the library of TLAPS*.
Some theorems from the module FiniteSetTheorems can be found also in the module NaiadClockProofFiniteSets[1, *C*.5 *on p*.57].

Author : *Ioannis Filippidis*

Reference

[1] *Thomas L.Rodeheffer*
"*The Naiad Clock Protocol* :
Specification, *Model Checking*, *and Correctness Proof*"
MSR − *TR* − 2013 − 20, *Microsoft Research*, *Silicon Valley*, 2013

EXTENDS
FiniteSetTheorems,
Naturals

In order to ensure independence from builtin support of Sequences by TLAPS, *these modules have been developed and checked by replacing the modules FiniteSets*, *FiniteSetTheorems*, *Sequences*, *SequencesTheorems with renamed copies*, (*FiniteSets_copy etc.*), *and appropriately adjusting* EXTENDS *statements where needed*.

Special case of FS_Union
COROLLARY $FS\_UnionDisjoint \triangleq$
ASSUME
NEW S, NEW T,
$\land IsFiniteSet(S) \land IsFiniteSet(T)$
$\land (S \cap T) = \{\}$
PROVE
$Cardinality(S \cup T) = Cardinality(S) + Cardinality(T)$
PROOF
$\langle 1 \rangle 1.\ Cardinality(S \cup T) =$
$Cardinality(S) + Cardinality(T) - Cardinality(S \cap T)$
BY FS_Union
$\langle 1 \rangle 2.\ Cardinality(S \cap T) = 0$
BY $FS\_EmptySet$
$\langle 1 \rangle$ QED
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $FS\_CardinalityType$

A corollary of FS_AddElement.
COROLLARY $FS\_AddElementUpperBound \triangleq$
ASSUME
NEW S, NEW x,

$IsFiniteSet(S)$
PROVE
LET $Q \triangleq S \cup \{x\}$
IN $\land IsFiniteSet(Q)$
$\land Cardinality(Q) \leq Cardinality(S) + 1$
PROOF
$\langle 1 \rangle$ DEFINE $Q \triangleq S \cup \{x\}$
$\langle 1 \rangle 1$. $IsFiniteSet(S)$
OBVIOUS
$\langle 1 \rangle 2$. $\land IsFiniteSet(Q)$
$\land \lor Cardinality(Q) = Cardinality(S)$
$\lor Cardinality(Q) = Cardinality(S) + 1$
BY $\langle 1 \rangle 1$, $FS\_AddElement$
$\langle 1 \rangle 3$. $\land Cardinality(Q) \in Nat$
$\land Cardinality(S) \in Nat$
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $FS\_CardinalityType$
$\langle 1 \rangle$ QED
BY $\langle 1 \rangle 2$, $\langle 1 \rangle 3$

Using this lemma directly works well.
LEMMA $ImageOfFinite \triangleq$
ASSUME
NEW S, NEW $Op(\_)$,
$IsFiniteSet(S)$
PROVE
LET
$Img \triangleq \{Op(x) : x \in S\}$
IN
$\land IsFiniteSet(Img)$
$\land Cardinality(Img) \leq Cardinality(S)$
PROOF
$\langle 1 \rangle$ DEFINE
$Img \triangleq \{Op(x) : x \in S\}$
$f \triangleq [x \in S \mapsto Op(x)]$
$\langle 1 \rangle 1$. $f \in Surjection(S, Img)$
BY DEF $Surjection$
$\langle 1 \rangle$ QED
BY $\langle 1 \rangle 1$, $FS\_Surjection$

COROLLARY $ImageOfFinite2 \triangleq$
ASSUME
NEW S, NEW $arg2$, NEW $Op(\_, \_)$,
$IsFiniteSet(S)$
PROVE

LET
$Img \triangleq \{Op(x,\ arg2) :\ x \in S\}$
IN
$\land\ IsFiniteSet(Img)$
$\land\ Cardinality(Img) \leq Cardinality(S)$
PROOF
BY $ImageOfFinite$

COROLLARY $ImageOfFinite3 \triangleq$
ASSUME
NEW S, NEW $arg2$, NEW $arg3$, NEW $Op(\_,\ \_,\ \_)$,
$IsFiniteSet(S)$
PROVE
LET
$Img \triangleq \{Op(x,\ arg2,\ arg3) :\ x \in S\}$
IN
$\land\ IsFiniteSet(Img)$
$\land\ Cardinality(Img) \leq Cardinality(S)$
PROOF
BY $ImageOfFinite$

(∗ *Proofs checked with TLAPS version* 1.4.3 ∗)

MODULE *Optimization*

Generic notions of optimization and binary relations as functions.

- minimal, maximal, minimum, maximum elements
- reflexive, irreflexive, transitive, symmetric, antisymmetric relations
– *antichains*, chains
- properties of the above

Author: Ioannis *Filippidis*

EXTENDS

FiniteSetFacts,
Integers,
WellFoundedInduction

$IsAFunction(f) \triangleq f = [x \in \text{DOMAIN } f \mapsto f[x]]$

$Support(R) \triangleq \{p[1] : p \in \text{DOMAIN } R\} \cup \{p[2] : p \in \text{DOMAIN } R\}$

$IsReflexive(R) \triangleq \text{LET } S \triangleq Support(R)$
$\text{IN } \forall x \in S : R[x, x]$

$IsIrreflexive(R) \triangleq \text{LET } S \triangleq Support(R)$
$\text{IN } \forall x \in S : \neg R[x, x]$

$IsTransitive(R) \triangleq \text{LET } S \triangleq Support(R)$
$\text{IN } \forall x, y, z \in S : (R[x, y] \land R[y, z]) \Rightarrow R[x, z]$

$IsSymmetric(R) \triangleq \text{LET } S \triangleq Support(R)$
$\text{IN } \forall x, y \in S : R[x, y] \Rightarrow R[y, x]$

$IsAntiSymmetric(R) \triangleq \text{LET } S \triangleq Support(R)$
$\text{IN } \forall x, y \in S : (R[x, y] \land (x \neq y)) \Rightarrow \neg R[y, x]$

S is a set of pairwise comparable elements(totality).
$IsChain(S, Leq) \triangleq \forall x, y \in S : Leq[x, y] \lor Leq[y, x]$

S is a set of pairwise incomparable elements.
$IsAntiChain(S, Leq) \triangleq \forall x, y \in S :$
$(x \neq y) \Rightarrow (\neg Leq[x, y] \land \neg Leq[y, x])$

Optimization

When the minimum exists, it is unique, similarly for the maximum.
$IsMinimum(r, S, Leq) \triangleq \land r \in S$
$\land \forall u \in S \setminus \{r\} : Leq[r, u]$

$$IsMaximum(r,\ S,\ Leq) \triangleq \begin{array}{l} \land\ r \in S \\ \land\ \forall\, u \in S \setminus \{r\} :\ Leq[u,\ r] \end{array}$$

This definition requires that Leq be reflexive, so it applies to partial orders.

$$IsMinimalRefl(r,\ S,\ Leq) \triangleq \begin{array}{l} \land\ r \in S \\ \land\ \forall\, u \in S \setminus \{r\} :\ \neg Leq[u,\ r] \end{array}$$

$$IsMaximalRefl(r,\ S,\ Leq) \triangleq \begin{array}{l} \land\ r \in S \\ \land\ \forall\, u \in S \setminus \{r\} :\ \neg Leq[r,\ u] \end{array}$$

Most general definition, applies even if Leq is not anti − symmetric, so also to preorders.

$$IsMinimal(r,\ S,\ Leq) \triangleq \begin{array}{l} \land\ r \in S \\ \land\ \forall\, u \in S :\ Leq[u,\ r] \Rightarrow Leq[r,\ u] \end{array}$$

$$IsMaximal(r,\ S,\ Leq) \triangleq \begin{array}{l} \land\ r \in S \\ \land\ \forall\, u \in S :\ Leq[r,\ u] \Rightarrow Leq[u,\ r] \end{array}$$

This definition is used in the implementation, because the BDD of Eq[u, r]turns out to be(much)smaller than the BDD of Leq[r, u].

$$IsAMinimumAlt(r,\ S,\ Leq,\ Eq) \triangleq \begin{array}{l} \land\ r \in S \\ \land\ \forall\, u \in S :\ Leq[u,\ r] \Rightarrow Eq[u,\ r] \end{array}$$

If a minimum does exist, then it is unique, so clearly "minima" *refers to minimal elements.In presence of the minimum, Minima is a singleton.*

$$Minima(S,\ Leq) \triangleq \{x \in S :\ IsMinimal(x,\ S,\ Leq)\}$$
$$Maxima(S,\ Leq) \triangleq \{x \in S :\ IsMaximal(x,\ S,\ Leq)\}$$

$$IndicatorFuncToRel(f) \triangleq \{x \in \text{DOMAIN } f :\ f[x] = \text{TRUE}\}$$
$$IrreflexiveFrom(Leq) \triangleq$$
LET
$S \triangleq Support(Leq)$
IN
$[t \in S \times S \mapsto \text{IF } t[1] = t[2] \text{ THEN FALSE ELSE } Leq[t]]$

Definition of IsMaximal restated as a theorem.

LEMMA $MaxProperties \triangleq$
ASSUME
NEW Leq, NEW S, NEW x, NEW $other$,
$IsMaximal(x,\ S,\ Leq)$
PROVE
$\land\ x \in S$
$\land\ (other \in S\ \land\ Leq[x,\ other]) \Rightarrow Leq[other,\ x]$

PROOF
BY DEF *IsMaximal*

COROLLARY *MaximaProperties* $\triangleq$
ASSUME
NEW *Leq*, NEW *S*, NEW *x*, NEW *other*,
$x \in Maxima(S, Leq)$
PROVE
$\land x \in S$
$\land (other \in S \ \land \ Leq[x, other]) \Rightarrow Leq[other, x]$
PROOF
BY *MaxProperties* DEF *Maxima*

THEOREM *MaxIsIdempotent* $\triangleq$
ASSUME NEW *S*, NEW *Leq*
PROVE LET $Max(Q) \triangleq Maxima(Q, Leq)$
IN $Max(Max(S)) = Max(S)$
PROOF
BY DEF *Maxima*, *IsMaximal*

THEOREM *MaxIsSubset* $\triangleq$
ASSUME NEW *S*, NEW *Leq*
PROVE $Maxima(S, Leq) \subseteq S$
PROOF
BY DEF *Maxima*

THEOREM *MaxSmaller* $\triangleq$
ASSUME
NEW *S*, NEW *Leq*,
$IsFiniteSet(S)$
PROVE
LET
$Max \triangleq Maxima(S, Leq)$
IN
$\land IsFiniteSet(Max)$
$\land Cardinality(Max) \leq Cardinality(S)$
PROOF
BY *MaxIsSubset*, *FS_Subset*

S = Max(S) when S is an antichain.
THEOREM *MaxSame* $\triangleq$
ASSUME
NEW *S*, NEW *Leq*,

IsFiniteSet(*S*),
Cardinality(*S*) = *Cardinality*(*Maxima*(*S*, *Leq*))
PROVE
S = *Maxima*(*S*, *Leq*)
PROOF
⟨1⟩ DEFINE
Max ≜ *Maxima*(*S*, *Leq*)
Card(*R*) ≜ *Cardinality*(*R*)
⟨1⟩1. SUFFICES ASSUME *S* ≠ *Max*
PROVE FALSE
OBVIOUS
⟨1⟩2. ∧ *Max* ⊆ *S*
∧ *Max* ≠ *S*
BY *MaxIsSubset*, ⟨1⟩1
⟨1⟩3. *Card*(*Max*) < *Card*(*S*)
BY ⟨1⟩2, *FS_Subset*
⟨1⟩ QED
BY ⟨1⟩3

THEOREM *MaximaIsAntiChain* ≜
ASSUME
NEW *S*, NEW *Leq*,
IsAntiSymmetric(*Leq*),
S ⊆ *Support*(*Leq*),
S = *Maxima*(*S*, *Leq*)
PROVE
IsAntiChain(*S*, *Leq*)
PROOF
⟨1⟩1. SUFFICES ASSUME NEW *x* ∈ *S*, NEW *y* ∈ *S*,
∧ *x* ≠ *y*
∧ *Leq*[*x*, *y*]
PROVE FALSE
BY DEF *IsAntiChain*
⟨1⟩2. ¬*Leq*[*y*, *x*]
BY ⟨1⟩1 DEF *IsAntiSymmetric*
⟨1⟩3. *Leq*[*y*, *x*]
⟨2⟩1. *IsMaximal*(*x*, *S*, *Leq*)
BY ⟨1⟩1 DEF *Maxima*
⟨2⟩ QED
BY ⟨1⟩1, ⟨2⟩1 DEF *IsMaximal*
⟨1⟩ QED
BY ⟨1⟩2, ⟨1⟩3

THEOREM *AntiChainIsMaxima* ≜

ASSUME
NEW S, NEW Leq,
$\land\ IsReflexive(Leq)$
$\land\ IsAntiChain(S,\ Leq)$
PROVE
$S = Maxima(S,\ Leq)$
PROOF
$\langle 1\rangle 1$. SUFFICES ASSUME NEW $x \in S$, NEW $y \in S$,
$Leq[y,\ x]$
PROVE $Leq[x,\ y]$
BY DEF $Maxima$, $IsMaximal$
$\langle 1\rangle 2$.CASE $x = y$
BY $\langle 1\rangle 1$, $\langle 1\rangle 2$ DEF $IsReflexive$
$\langle 1\rangle 3$.CASE $x \neq y$
BY $\langle 1\rangle 1$, $\langle 1\rangle 3$ DEF $IsAntiChain$
$\langle 1\rangle$ QED
BY $\langle 1\rangle 2$, $\langle 1\rangle 3$

THEOREM $EquivDefsOfMin \triangleq$
ASSUME NEW S, NEW Leq, NEW Eq,
$\forall\, u,\ r \in S :\ Eq[u,\ r] \equiv (Leq[u,\ r] \land Leq[r,\ u])$
PROVE $\forall\, r \in S :$
$IsMinimal(r,\ S,\ Leq) \equiv IsAMinimumAlt(r,\ S,\ Leq,\ Eq)$
PROOF
BY DEF $IsMinimal$, $IsAMinimumAlt$

If $x \in S$(so S is nonempty), and x is not a minimum, then some $y \in S \setminus \{x\}$is smaller than x.

THEOREM $SmallerExists \triangleq$
ASSUME
NEW Leq, NEW S, NEW $x \in S$,
$\neg IsMinimal(x,\ S,\ Leq)$
PROVE
$\exists\, y \in S :\ \land\ y \neq x$
$\land\ Leq[y,\ x]$
$\land\ \neg Leq[x,\ y]$
PROOF
BY DEF $IsMinimal$

THEOREM $LargerExists \triangleq$
ASSUME
NEW Leq, NEW S, NEW $x \in S$,
$\neg IsMaximal(x,\ S,\ Leq)$
PROVE

$$\exists\, y \in S : \ \begin{array}{l} \land\ y \neq x \\ \land\ Leq[x,\ y] \\ \land\ \neg Leq[y,\ x] \end{array}$$

PROOF
BY DEF *IsMaximal*

THEOREM *StrictSubsetOfFiniteWellFoundedOnSubsets* $\triangleq$
ASSUME
NEW S,
IsFiniteSet(S)
PROVE
LET
LeqRel $\triangleq$ *StrictSubsetOrdering*(S)
IN
IsWellFoundedOn(*LeqRel*, SUBSET S)
PROOF
BY *FS_StrictSubsetOrderingWellFounded*, *FS_FiniteSubsetsOfFinite*

PROPOSITION *IndicatorTrueOnRel* $\triangleq$
ASSUME
NEW f
PROVE
$\forall\, x \in$ *IndicatorFuncToRel*(f) : $f[x]$
PROOF
BY DEF *IndicatorFuncToRel*

PROPOSITION *IndicatorEquivRel* $\triangleq$
ASSUME
NEW f, NEW x
PROVE
LET $R \triangleq$ *IndicatorFuncToRel*(f)
IN $(x \in R) \equiv \begin{array}{l} \land\ x \in \text{DOMAIN } f \\ \land\ f[x] \end{array}$
PROOF
BY DEF *IndicatorFuncToRel*

PROPOSITION *SupportOfSymmetricDomain* $\triangleq$
ASSUME
NEW *Leq*, NEW S,
(DOMAIN *Leq*) $= (S \times S)$
PROVE
$S =$ *Support*(*Leq*)

PROOF
⟨1⟩ DEFINE $Z \triangleq Support(Leq)$
⟨1⟩1. $Z \subseteq S$
BY DEF *Support*
⟨1⟩2. $S \subseteq Z$
⟨3⟩ SUFFICES ASSUME NEW $u \in S$
PROVE $u \in Z$
OBVIOUS
⟨3⟩ QED
BY DEF *Support*
⟨1⟩ QED
BY ⟨1⟩1, ⟨1⟩2

PROPOSITION *LtDomainIsSupportSquared* $\triangleq$
ASSUME
NEW *Leq*
PROVE
LET
$Lt \triangleq IrreflexiveFrom(Leq)$
$S \triangleq Support(Lt)$
IN $(S \times S) = \text{DOMAIN } Lt$
PROOF
⟨1⟩ DEFINE $Lt \triangleq IrreflexiveFrom(Leq)$
⟨1⟩1. PICK $S : (S \times S) = \text{DOMAIN } Lt$
BY DEF *IrreflexiveFrom*
⟨1⟩2. $S = Support(Lt)$
BY ⟨1⟩1, *SupportOfSymmetricDomain*
⟨1⟩ QED
BY ⟨1⟩1, ⟨1⟩2

PROPOSITION *LtHasSameSupport* $\triangleq$
ASSUME
NEW *Leq*
PROVE
LET $Lt \triangleq IrreflexiveFrom(Leq)$
IN $Support(Lt) = Support(Leq)$
PROOF
⟨1⟩ DEFINE
$Z \triangleq Support(Leq)$
$Lt \triangleq IrreflexiveFrom(Leq)$
⟨1⟩1. $Support(Lt) \subseteq Z$
BY DEF *IrreflexiveFrom*, *Support*
⟨1⟩2. $Z \subseteq Support(Lt)$
⟨2⟩1. $\forall\, u \in Z : \exists\, p \in \text{DOMAIN } Lt : p[1] = u$

```
        BY  DEF IrreflexiveFrom
    ⟨2⟩2. Z ⊆ {p[1] : p ∈ DOMAIN Lt}
        BY ⟨2⟩1
    ⟨2⟩ QED
        BY ⟨2⟩2  DEF Support
⟨1⟩ QED
    BY ⟨1⟩1, ⟨1⟩2

PROPOSITION LtHasSameDomain ≜
  ASSUME
    NEW Leq,
    ∃ S : DOMAIN Leq = (S × S)
  PROVE
    LET Lt ≜ IrreflexiveFrom(Leq)
    IN  DOMAIN Leq = DOMAIN Lt
  PROOF
  ⟨1⟩ DEFINE
      Z ≜ Support(Leq)
      Lt ≜ IrreflexiveFrom(Leq)
  ⟨1⟩1. PICK S : DOMAIN Leq = (S × S)
      OBVIOUS
  ⟨1⟩2. S = Z
      ⟨2⟩1. ASSUME NEW u ∈ S
                   PROVE u ∈ Z
          BY ⟨1⟩1  DEF Support
      ⟨2⟩2. ASSUME NEW u ∈ Z
                   PROVE u ∈ S
          ⟨3⟩1. PICK p ∈ DOMAIN Leq : ∨ p[1] = u
                                      ∨ p[2] = u
              BY  DEF Support
          ⟨3⟩2. ∧ p[1] ∈ S
                ∧ p[2] ∈ S
              BY ⟨1⟩1
          ⟨3⟩ QED
              BY ⟨3⟩1, ⟨3⟩2
      ⟨2⟩ QED
          BY ⟨2⟩1, ⟨2⟩2
  ⟨1⟩3. DOMAIN Lt = (Z × Z)
      BY LtHasSameSupport DEF IrreflexiveFrom
  ⟨1⟩ QED
      BY ⟨1⟩1, ⟨1⟩2, ⟨1⟩3

PROPOSITION LtIsIrreflexive ≜
  ASSUME
```

```
        NEW Leq
    PROVE
        LET Lt ≜ IrreflexiveFrom(Leq)
        IN  IsIrreflexive(Lt)
    PROOF
    ⟨1⟩ DEFINE
        Z ≜ Support(Leq)
        Lt ≜ IrreflexiveFrom(Leq)
    ⟨1⟩1. SUFFICES ASSUME NEW x ∈ Z
                   PROVE ¬Lt[x, x]
        ⟨2⟩ Support(Lt) = Support(Leq)
            BY LtHasSameSupport
        ⟨2⟩ QED
            BY ⟨1⟩1 DEF IsIrreflexive
    ⟨1⟩2. ⟨x, x⟩ ∈ Z × Z
        BY ⟨1⟩1
    ⟨1⟩ QED
        BY ⟨1⟩2 DEF IrreflexiveFrom

PROPOSITION LtIsTransitive ≜
    ASSUME
        NEW Leq,
        ∧ IsAntiSymmetric(Leq)
        ∧ IsTransitive(Leq)
    PROVE
        LET Lt ≜ IrreflexiveFrom(Leq)
        IN  IsTransitive(Lt)
    PROOF
    ⟨1⟩ DEFINE
        Lt ≜ IrreflexiveFrom(Leq)
        Z ≜ Support(Leq)
        W ≜ Support(Lt)
    ⟨1⟩1. Z = W
        BY LtHasSameSupport
    ⟨1⟩2. ASSUME NEW x ∈ W, NEW y ∈ W
          PROVE ⟨x, y⟩ ∈ DOMAIN Lt
        ⟨2⟩ (W × W) = DOMAIN Lt
            BY LtDomainIsSupportSquared
        ⟨2⟩ ⟨x, y⟩ ∈ (W × W)
            OBVIOUS
        ⟨2⟩ QED
            OBVIOUS
    ⟨1⟩3. SUFFICES ASSUME NEW x ∈ W, NEW y ∈ W, NEW z ∈ W,
                           Lt[x, y] ∧ Lt[y, z]
```

PROVE $Lt[x, z]$
BY $\langle 1 \rangle 3$ DEF *IsTransitive*
$\langle 1 \rangle 4$. $x \neq y$
$\langle 2 \rangle 1$. SUFFICES ASSUME $x = y$
PROVE FALSE
OBVIOUS
$\langle 2 \rangle 2$. $\langle x, x \rangle \in$ DOMAIN Lt
BY $\langle 1 \rangle 2$
$\langle 2 \rangle 3$. $Lt[x, x]$
BY $\langle 1 \rangle 3$, $\langle 2 \rangle 1$
$\langle 2 \rangle$ QED
BY $\langle 2 \rangle 2$, $\langle 2 \rangle 3$ DEF *IrreflexiveFrom*
$\langle 1 \rangle 5$. $Leq[x, y]$
$\langle 2 \rangle 1$. $\langle x, y \rangle \in$ DOMAIN Lt
BY $\langle 1 \rangle 2$
$\langle 2 \rangle 2$. $Lt[x, y]$
BY $\langle 1 \rangle 3$
$\langle 2 \rangle$ QED
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$ DEF *IrreflexiveFrom*
$\langle 1 \rangle 6$. $Leq[y, z]$
$\langle 2 \rangle 1$. $\langle y, z \rangle \in$ DOMAIN Lt
BY $\langle 1 \rangle 2$
$\langle 2 \rangle 2$. $Lt[y, z]$
BY $\langle 1 \rangle 3$
$\langle 2 \rangle$ QED
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$ DEF *IrreflexiveFrom*
$\langle 1 \rangle 7$. $Leq[x, z]$
$\langle 2 \rangle 1$. $\land x \in Z$
$\land y \in Z$
$\land z \in Z$
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 3$
$\langle 2 \rangle$ QED
BY $\langle 2 \rangle 1$, $\langle 1 \rangle 5$, $\langle 1 \rangle 6$ DEF *IsTransitive*
$\langle 1 \rangle$ QED
$\langle 2 \rangle 1$. $\langle x, z \rangle \in$ DOMAIN Lt
BY $\langle 1 \rangle 2$
$\langle 2 \rangle 2$. $x \neq z$
$\langle 3 \rangle 1$. SUFFICES ASSUME $x = z$
PROVE FALSE
OBVIOUS
$\langle 3 \rangle 2$. $Leq[x, y] \land Leq[y, x]$
BY $\langle 1 \rangle 5$, $\langle 1 \rangle 6$, $\langle 3 \rangle 1$
$\langle 3 \rangle 3$. $\neg Leq[y, x]$
$\langle 4 \rangle 1$. $(x \in Z) \land (y \in Z)$
BY $\langle 1 \rangle 3$, $\langle 1 \rangle 1$

```
                ⟨4⟩2. x ≠ y
                    BY ⟨1⟩4
                ⟨4⟩3. Leq[x, y]
                    BY ⟨3⟩2
                ⟨4⟩ QED
                    BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3 DEF IsAntiSymmetric
            ⟨3⟩ QED
                BY ⟨3⟩2, ⟨3⟩3
        ⟨2⟩ QED
            BY ⟨2⟩1, ⟨2⟩2, ⟨1⟩7 DEF IrreflexiveFrom

PROPOSITION FiniteLatticeInducesWellFounded ≜
    ASSUME
        NEW Leq, NEW S,
        LET
            Z ≜ Support(Leq)
        IN
            ∧ IsFiniteSet(S)
            ∧ IsTransitive(Leq)
            ∧ IsAntiSymmetric(Leq)
            ∧ S ⊆ Z
    PROVE
        LET
            Z ≜ Support(Leq)
            Lt ≜ IrreflexiveFrom(Leq)
            R ≜ IndicatorFuncToRel(Lt)
        IN
            IsWellFoundedOn(R, S)
    PROOF
    ⟨1⟩ DEFINE
        Z ≜ Support(Leq)
        Lt ≜ IrreflexiveFrom(Leq)
        W ≜ Support(Lt)
        R ≜ IndicatorFuncToRel(Lt)
    ⟨1⟩1. IsIrreflexive(Lt)
        BY LtIsIrreflexive
    ⟨1⟩2. IsTransitive(Lt)
        BY LtIsTransitive
    ⟨1⟩3. ∀ x ∈ Z : ⟨x, x⟩ ∉ R
        ⟨2⟩1. SUFFICES ASSUME NEW x ∈ Z
                       PROVE ⟨x, x⟩ ∉ R
            OBVIOUS
        ⟨2⟩2. ¬Lt[x, x]
            ⟨3⟩ ⟨x, x⟩ ∈ (Z × Z)
```

OBVIOUS

⟨3⟩ QED
BY DEF *IrreflexiveFrom*

⟨2⟩ QED
BY ⟨2⟩2 DEF *IndicatorFuncToRel*

⟨1⟩4. SUFFICES ASSUME $\neg IsWellFoundedOn(R, S)$
PROVE FALSE
OBVIOUS

⟨1⟩5. PICK $f \in [Nat \to S]$:
$\forall\, n \in Nat : \langle f[n+1], f[n]\rangle \in R$
BY ⟨1⟩4 DEF *IsWellFoundedOn*

⟨1⟩6. $\forall\, n \in Nat : f[n] \in W$
BY ⟨1⟩5, *LtHasSameSupport*

⟨1⟩7. ASSUME NEW $i \in Nat$, NEW $j \in Nat$,
$i < j$
PROVE $\langle f[j], f[i]\rangle \in R$

⟨2⟩1. $\forall\, n \in Nat : Lt[f[n+1], f[n]]$
BY ⟨1⟩5, *IndicatorEquivRel*

⟨2⟩2. $\forall\, n \in Nat : Lt[f[i+n+1], f[i]]$

⟨3⟩1. $Lt[f[i+1], f[i]]$
BY ⟨2⟩1, ⟨1⟩7

⟨3⟩2. ASSUME NEW $n \in Nat$,
$Lt[f[i+n+1], f[i]]$
PROVE $Lt[f[i+n+2], f[i]]$

⟨4⟩1. $k \triangleq i+n+1$

⟨4⟩2. $Lt[f[k+1], f[k]]$
BY ⟨2⟩1, ⟨3⟩2

⟨4⟩3. $Lt[f[k], f[i]]$
BY ⟨3⟩2

⟨4⟩4. SUFFICES $Lt[f[k+1], f[i]]$
OBVIOUS

⟨4⟩5. $\wedge\, f[k] \in W$
$\wedge\, f[k+1] \in W$
$\wedge\, f[i] \in W$
BY ⟨1⟩6

⟨4⟩ QED
BY ⟨4⟩2, ⟨4⟩3, ⟨4⟩5, ⟨1⟩2 DEF *IsTransitive*

⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, *NatInduction*

⟨2⟩3. $Lt[f[i+(j-i-1)+1], f[i]]$

⟨3⟩1. $n \triangleq j-i-1$

⟨3⟩2. $n \in Nat$
BY ⟨1⟩7

⟨3⟩3. $Lt[f[i+n+1], f[i]]$
BY ⟨3⟩2, ⟨2⟩2

⟨3⟩ QED
BY ⟨3⟩3
⟨2⟩4. $Lt[f[j], f[i]]$
BY ⟨1⟩7, ⟨2⟩3
⟨2⟩5. $\langle f[j], f[i]\rangle \in$ DOMAIN Lt
⟨3⟩ $\langle f[j], f[i]\rangle \in (W \times W)$
BY ⟨1⟩6
⟨3⟩ $W = Z$
BY *LtHasSameSupport*
⟨3⟩ QED
BY *LtDomainIsSupportSquared*
⟨2⟩ QED
BY ⟨2⟩4, ⟨2⟩5, *IndicatorEquivRel*
⟨1⟩8. $\forall\, i, j \in Nat :\ (i \neq j) \Rightarrow (f[i] \neq f[j])$
⟨2⟩1. SUFFICES ASSUME NEW $i \in Nat$, NEW $j \in Nat$, $i < j$ PROVE $f[i] \neq f[j]$
OBVIOUS
⟨2⟩2. $\langle f[j], f[i]\rangle \in R$
BY ⟨2⟩1, ⟨1⟩7
⟨2⟩ QED
BY ⟨2⟩2, ⟨1⟩6, ⟨1⟩3, *LtHasSameSupport*
⟨1⟩9. PICK $k \in Nat :\ k = Cardinality(S)$
BY *FS_CardinalityType*
⟨1⟩ DEFINE
$m \triangleq k + 1$
$D \triangleq 1 \,..\, m$
$T \triangleq \{f[n] :\ n \in D\}$
⟨1⟩10. $\forall\, i, j \in D :\ (i \neq j) \Rightarrow f[i] \neq f[j]$
BY ⟨1⟩9, ⟨1⟩8
⟨1⟩11. $ExistsBijection(D,\ T)$
⟨2⟩1. $g \triangleq [n \in D \mapsto f[n]]$
⟨2⟩2. $g \in [D \to T]$
OBVIOUS
⟨2⟩3. $g \in Injection(D,\ T)$
BY ⟨1⟩10 DEF *Injection*
⟨2⟩4. $g \in Surjection(D,\ T)$
BY DEF *Surjection*
⟨2⟩5. $g \in Bijection(D,\ T)$
BY ⟨2⟩3, ⟨2⟩4 DEF *Bijection*
⟨2⟩ QED
BY ⟨2⟩5 DEF *ExistsBijection*
⟨1⟩12. $\wedge\, IsFiniteSet(T)$
$\wedge\, m = Cardinality(T)$
BY ⟨1⟩11, *FS_NatBijection*, *FS_CountingElements*

⟨1⟩13. $\land\ T \subseteq S$
$\land\ T \neq S$
BY ⟨1⟩8
⟨1⟩14. $Cardinality(T) < Cardinality(S)$
⟨2⟩1. $\land\ Cardinality(T) \leq Cardinality(S)$
$\land\ (Cardinality(T) = Cardinality(S)) \Rightarrow (S = T)$
BY ⟨1⟩13, FS_Subset
⟨2⟩ QED
BY ⟨2⟩1, ⟨1⟩13
⟨1⟩ QED
⟨2⟩1. $m < k$
BY ⟨1⟩9, ⟨1⟩12, ⟨1⟩14
⟨2⟩ QED
BY ⟨2⟩1

THEOREM $FiniteSetHasMinimal \triangleq$
ASSUME
NEW Leq, NEW S,
LET
$Z \triangleq Support(Leq)$
IN
$\land\ IsTransitive(Leq)$
$\land\ IsAntiSymmetric(Leq)$
$\land\ IsFiniteSet(S)$
$\land\ S \subseteq Z$
$\land\ S \neq \{\}$
PROVE
$\exists\, v \in S :\ IsMinimal(v, S, Leq)$
PROOF
⟨1⟩ DEFINE
$Z \triangleq Support(Leq)$
$Lt \triangleq IrreflexiveFrom(Leq)$
$W \triangleq Support(Lt)$
$R \triangleq IndicatorFuncToRel(Lt)$
⟨1⟩1. $S \subseteq W$
BY $LtHasSameSupport$
⟨1⟩2. $IsWellFoundedOn(R, S)$
BY $FiniteLatticeInducesWellFounded$
⟨1⟩3. PICK $v \in S :\ \forall\, u \in S :\ \langle u, v\rangle \notin R$
BY ⟨1⟩2, $WFMin$
⟨1⟩4. $\forall\, u \in S :\ \neg Lt[u, v]$
⟨2⟩1. SUFFICES ASSUME NEW $u \in S$
PROVE $\neg Lt[u, v]$
OBVIOUS

⟨2⟩2. $\land\ u \in W$
$\land\ v \in W$
BY ⟨1⟩3, ⟨2⟩1, ⟨1⟩1
⟨2⟩3. $\langle u,\ v\rangle \notin R$
BY ⟨1⟩3
⟨2⟩4. $\langle u,\ v\rangle \in$ DOMAIN Lt
⟨3⟩ $\langle u,\ v\rangle \in (W \times W)$
BY ⟨2⟩2
⟨3⟩ QED
BY *LtDomainIsSupportSquared*
⟨2⟩ QED
BY ⟨2⟩3, ⟨2⟩4, *IndicatorEquivRel*
⟨1⟩5. $\forall\, u \in S \setminus \{v\} :\ \neg Leq[u,\ v]$
⟨2⟩ SUFFICES ASSUME NEW $u \in S \setminus \{v\}$
PROVE $\neg Leq[u,\ v]$
OBVIOUS
⟨2⟩1. $\langle u,\ v\rangle \in Z \times Z$
BY ⟨1⟩1, *LtHasSameSupport*
⟨2⟩2. $Lt[u,\ v] = Leq[u,\ v]$
BY ⟨2⟩1 DEF *IrreflexiveFrom*
⟨2⟩ QED
BY ⟨1⟩4, ⟨2⟩2
⟨1⟩ QED
BY ⟨1⟩5 DEF *IsMinimal*

THEOREM *HasSomeMinimalBelow* $\triangleq$
ASSUME
NEW *Leq*, NEW S, NEW $u \in S$,
LET
$Z \triangleq Support(Leq)$
IN
$\land\ IsFiniteSet(Z)$
$\land\ IsReflexive(Leq)$
$\land\ IsTransitive(Leq)$
$\land\ IsAntiSymmetric(Leq)$
$\land\ S \subseteq Z$
PROVE
$\exists\, v \in S :\ \land\ Leq[v,\ u]$
$\land\ IsMinimal(v,\ S,\ Leq)$
PROOF
⟨1⟩ DEFINE
$R \triangleq \{r \in S :\ Leq[r,\ u]\}$
$Z \triangleq Support(Leq)$
⟨1⟩1. $u \in R$

BY DEF *IsReflexive*

⟨1⟩2. *IsFiniteSet*(*R*)
BY *FS_Subset* DEF *R*

⟨1⟩3. PICK $v \in R$: *IsMinimal*(*v*, *R*, *Leq*)
BY ⟨1⟩1, ⟨1⟩2, *FiniteSetHasMinimal*

⟨1⟩4. SUFFICES *IsMinimal*(*v*, *S*, *Leq*)
⟨2⟩1. *Leq*[*v*, *u*]
BY ⟨1⟩3 DEF *R*
⟨2⟩ QED
BY ⟨2⟩1

⟨1⟩5. SUFFICES ASSUME ¬*IsMinimal*(*v*, *S*, *Leq*)
PROVE FALSE
OBVIOUS

⟨1⟩6. PICK $w \in S \setminus \{v\}$: $\land$ *Leq*[*w*, *v*]
$\land \neg$*Leq*[*v*, *w*]
BY ⟨1⟩5, *SmallerExists*

⟨1⟩7. $w \in R$
BY ⟨1⟩6, ⟨1⟩3 DEF *IsTransitive*

⟨1⟩ QED
BY ⟨1⟩3, ⟨1⟩7, ⟨1⟩6 DEF *IsMinimal*

(∗ *Proofs checked with TLAPS version* 1.4.3 ∗)

(∗
The definitions above use bounded quantifiers to enable using TLC. Also, sets instead of predicates reduce the amount of nesting in the definitions(flat is better than nested).The same definitions are possible using higher − order operators and unbounded quantifiers. These are given below.
∗)

(∗ *Defining IsMinimal and IsMaximal using Leq* ∗)

IsMinimal(*r*, *IsAMember*(_), *Leq*) $\triangleq$
$\land$ *IsAMember*(*r*)
$\land \forall u : \lor \neg$*IsAMember*(*u*)(∗ *outside the collection, or* ∗)
$\lor \neg$*Leq*[*u*, *r*](∗ *r no smaller than u, or* ∗)
$\lor$ *Leq*[*r*, *u*](∗ *r smaller than or equal to u* ∗)

IsAMinimumAlt(*r*, *IsAMember*(_), *Leq*, *Eq*) $\triangleq$
$\land$ *IsAMember*(*r*)
$\land \forall u : \lor \neg$*IsAMember*(*u*)
$\lor \neg$*Leq*[*u*, *r*]
$\lor$ *Eq*[*u*, *r*]

IsMaximal(*r*, *IsAMember*(_), *Leq*) $\triangleq$
$\land$ *IsAMember*(*r*)
$\land \forall u : \lor \neg$*IsAMember*(*u*)
$\lor \neg$*Leq*[*r*, *u*]

```
            ∨ Leq[u, r]

IsAMaximumAlt(r, IsAMember(_), Leq, Eq) ≜
    ∧ IsAMember(r)
    ∧ ∀ u : ∨ ¬IsAMember(u)
            ∨ ¬Leq[r, u]
            ∨ Eq[r, u]

(*
Design choices :

1.operator vs function for Leq
2.Leq as argument vs as CONSTANT
3.Leq vs Geq
4.expressing Min using Max
5.IsAMember as operator vs set containment
*)
```

```
(* Expressing IsMinimal using IsMaximal *)

IsMinimal(r, IsAMember, Leq) ≡
    ∧ IsAMember(r)
    ∧ ∀ u : ∨ ¬IsAMember(u)
            ∨ ¬Leq[u, r]
            ∨ Leq[r, u]
≡
   LET Geq[⟨a, b⟩ ∈ DOMAIN Leq] ≜ Leq[b, a]
   IN    ∧ IsAMember(r)
      ∧ ∀ u : ∨ ¬IsAMember(u)
              ∨ ¬Geq[r, u]
              ∨ Geq[u, r]
≡
   LET Geq[⟨a, b⟩ ∈ DOMAIN Leq] ≜ Leq[b, a]
   IN    IsMaximal(r, IsAMember, Geq)

(* The above indicates a possible alternative definition for IsMinimal. *)
```

```
(* Defining IsMinimal and IsMaximal using Geq *)

IsMinimal(r, IsAMember(_), Geq) ≜
    ∧ IsAMember(r)
    ∧ A u : ∨ ¬IsAMember(u)
            ∨ ¬Geq[r, u]
            ∨ Geq[u, r]

IsMaximal(r, IsAMember(_), Geq) ≜
    ∧ IsAMember(r)
    ∧ ∀ u : ∨ ¬IsAMember(u)
            ∨ ¬Geq[u, r]
            ∨ Geq[r, u]
```

```
(* Design note on defining maxima *)

THEOREM
```

$$
\begin{aligned}
\textsc{true} \equiv\ & \vee\ c \geq u \\
& \vee\ \neg(c \geq u) \\
\equiv\ & \vee\ c \geq u \\
& \vee\ \neg(c \geq u) \wedge \textsc{true} \\
\equiv\ & \vee\ c \geq u \\
& \vee\ \neg(c \geq u) \wedge\ \vee\ u \geq c \\
& \qquad\qquad \vee\ \neg(u \geq c) \\
\equiv\ & \vee\ c \geq u (*\ c\ \textit{at least as large as}\ u\ *) \\
& \vee\ \neg(c \geq u) \wedge (u \geq c) (*\ u\ \textit{strictly larger than}\ c\ *) \\
& \vee\ \neg(c \geq u) \wedge \neg(u \geq c) (*\ c\ \textit{and}\ u\ \textit{incomparable}\ *)
\end{aligned}
$$

$(*\ \textit{We want cases}\ 1\ \textit{and}\ 3\ \textit{only, so}\ *)$

$$
\begin{aligned}
& \vee\ c \geq u \\
& \vee\ \neg(c \geq u) \wedge \neg(u \geq c) \\
& \equiv \\
& \vee\ c \geq u \\
& \vee\ \neg(u \geq c)
\end{aligned}
$$

$(*\ \textit{It can also be shown that}:$

$$((p \leq q) \Rightarrow (p = q)) \equiv \neg(p \leq q \wedge p \neq q)$$

$*)$

MODULE *MinCover*

Definitions of minimal covering, and properties of minimal covers.

Author: Ioannis *Filippidis*

EXTENDS

Integers,
Optimization

CONSTANTS *Cost*

Minimal set covering

$$CostLeq[t \in (\text{DOMAIN } Cost) \times (\text{DOMAIN } Cost)] \triangleq$$
LET
$r \triangleq t[1]$
$u \triangleq t[2]$
IN $Cost[r] \leq Cost[u]$

$$CardinalityAsCost(Z) \triangleq Cost = [cover \in \text{SUBSET } Z \mapsto Cardinality(cover)]$$

C and X suffice to define a cover, because the notion of covering involves elements from a cover and a target set to cover. Y is irrelevant.

$$IsACover(C, X, IsUnder) \triangleq \forall x \in X : \exists y \in C : IsUnder[x, y]$$
$$IsACoverFrom(C, X, Y, IsUnder) \triangleq$$
$\wedge C \in \text{SUBSET } Y$
$\wedge IsACover(C, X, IsUnder)$
$$CoversOf(X, Y, IsUnder) \triangleq \{C \in \text{SUBSET } Y : IsACover(C, X, IsUnder)\}$$

The set Y is irrelevant to the notion of a cover, but is necessary to define a notion of minimal element.

$$IsAMinCover(C, X, Y, IsUnder) \triangleq$$
LET
$Covers \triangleq CoversOf(X, Y, IsUnder)$
IN
$IsMinimal(C, Covers, CostLeq)$

$$MinCost(X, Y, IsUnder) \triangleq$$
LET
$Cov \triangleq CoversOf(X, Y, IsUnder)$
$min \triangleq \text{CHOOSE } u \in Minima(Cov, CostLeq) : \text{TRUE}$
IN
$Cost[min]$

IsACover$(C,\ X,\ Leq) \equiv$ *Refines*$(X,\ C,\ Leq)$

$Refines(A,\ B,\ Leq) \triangleq \forall\, u \in A :\ \exists\, v \in B :\ Leq[u,\ v]$

The operator Refines from the module Lattices is equivalent to the operator IsACover from the module MinCover.

PROPOSITION *RefinesMeansCover* $\triangleq$

ASSUME
NEW A, NEW B, NEW Leq
PROVE
$Refines(A,\ B,\ Leq) \equiv IsACover(B,\ A,\ Leq)$

PROOF

$\langle 1\rangle 1$. ASSUME $Refines(A,\ B,\ Leq)$
PROVE $IsACover(B,\ A,\ Leq)$
$\langle 2\rangle 1$. $\forall\, u \in A :\ \exists\, v \in B :\ Leq[u,\ v]$
BY $\langle 1\rangle 1$ DEF *Refines*
$\langle 2\rangle 2$. $IsACover(B,\ A,\ Leq) =$
$\forall\, x \in A :\ \exists\, y \in B :\ Leq[x,\ y]$
BY DEF *IsACover*
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$

$\langle 1\rangle 2$. ASSUME $IsACover(B,\ A,\ Leq)$
PROVE $Refines(A,\ B,\ Leq)$
$\langle 2\rangle 1$. $\forall\, x \in A :\ \exists\, y \in B :\ Leq[x,\ y]$
BY $\langle 1\rangle 2$ DEF *IsACover*
$\langle 2\rangle 2$. $Refines(A,\ B,\ Leq) =$
$\forall\, u \in A :\ \exists\, v \in B :\ Leq[u,\ v]$
BY DEF *Refines*
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$

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

Transitivity of the operator Refines.

LEMMA *RefinesIsTransitive* $\triangleq$

ASSUME
NEW A, NEW B, NEW C, NEW Leq,
LET
$S \triangleq Support(Leq)$
IN
$\land\, A \subseteq S$
$\land\, B \subseteq S$
$\land\, C \subseteq S$
$\land\, IsTransitive(Leq)$
$\land\, Refines(A,\ B,\ Leq)$

$\land$ *Refines*(B, C, *Leq*)

PROVE

Refines(A, C, *Leq*)

PROOF

⟨1⟩ DEFINE

$S \triangleq$ *Support*(*Leq*)

⟨1⟩1. SUFFICES

ASSUME NEW $p \in A$

PROVE $\exists\, r \in C :$ *Leq*[p, r]

BY ⟨1⟩1 DEF *Refines*

⟨1⟩2. PICK $q \in B :$ *Leq*[p, q]

⟨2⟩1. *Refines*(A, B, *Leq*)

OBVIOUS

⟨2⟩ QED

BY ⟨1⟩1, ⟨2⟩1 DEF *Refines*

⟨1⟩3. PICK $r \in C :$ *Leq*[q, r]

⟨2⟩1. *Refines*(B, C, *Leq*)

OBVIOUS

⟨2⟩ QED

BY ⟨1⟩2, ⟨2⟩1 DEF *Refines*

⟨1⟩4. $\land\, p \in S$

$\land\, q \in S$

$\land\, r \in S$

⟨2⟩1. $\land\, A \subseteq S$

$\land\, B \subseteq S$

$\land\, C \subseteq S$

BY DEF S

⟨2⟩ QED

BY ⟨1⟩1, ⟨1⟩2, ⟨1⟩3, ⟨2⟩1

⟨1⟩5. *Leq*[p, q] $\land$ *Leq*[q, r]

BY ⟨1⟩2, ⟨1⟩3

⟨1⟩ QED

⟨2⟩1. *IsTransitive*(*Leq*)

OBVIOUS

⟨2⟩ QED

BY ⟨1⟩4, ⟨1⟩5, ⟨2⟩1 DEF *IsTransitive*

Transitivity of the operator IsACover.

COROLLARY *CoveringIsTransitive* $\triangleq$

ASSUME

NEW A, NEW B, NEW C, NEW *Leq*,

LET

$Z \triangleq$ *Support*(*Leq*)

IN

$\land A \subseteq Z$
$\land B \subseteq Z$
$\land C \subseteq Z$
$\land IsTransitive(Leq)$
$\land IsACover(A,\ B,\ Leq)$
$\land IsACover(B,\ C,\ Leq)$

PROVE
$IsACover(A,\ C,\ Leq)$

PROOF
BY $RefinesIsTransitive$, $RefinesMeansCover$

If S refines T, then any subset of S refines T.
PROPOSITION $SubsetRefinesToo \triangleq$
ASSUME
NEW S, NEW R, NEW T, NEW Leq,
$\land Refines(S,\ T,\ Leq)$
$\land R \in \text{SUBSET } S$
PROVE
$Refines(R,\ T,\ Leq)$
PROOF
$\langle 1\rangle 1.\ \forall u \in S :\ \exists v \in T :\ Leq[u,\ v]$
$\langle 2\rangle 1.\ Refines(S,\ T,\ Leq)$
OBVIOUS
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1$ DEF $Refines$
$\langle 1\rangle 2.\ \forall u \in R :\ u \in S$
OBVIOUS
$\langle 1\rangle 3.\ \forall u \in R :\ \exists v \in T :\ Leq[u,\ v]$
BY $\langle 1\rangle 1$, $\langle 1\rangle 2$
$\langle 1\rangle$ QED
BY $\langle 1\rangle 3$ DEF $Refines$

Auxiliary fact to aid TLAPS.
PROPOSITION $CostLeqHelper \triangleq$
$(\text{DOMAIN } CostLeq) = ((\text{DOMAIN } Cost) \times (\text{DOMAIN } Cost))$
PROOF
BY DEF $CostLeq$

Substitution of cardinality in the definition of CostLeq.
PROPOSITION $CostLeqToCard \triangleq$
ASSUME
NEW S,
NEW $A \in \text{SUBSET } S$,

```
        NEW B ∈ SUBSET S,
        CardinalityAsCost(S)
    PROVE
        CostLeq[⟨A, B⟩] = (Cardinality(A) ≤ Cardinality(B))
PROOF
⟨1⟩1. ∧ A ∈ SUBSET S
      ∧ B ∈ SUBSET S
    OBVIOUS
⟨1⟩2. Cost = [c ∈ SUBSET S ↦ Cardinality(c)]
    ⟨2⟩1. CardinalityAsCost(S)
        OBVIOUS
    ⟨2⟩ QED
        BY ⟨2⟩1 DEF CardinalityAsCost
⟨1⟩3. ⟨A, B⟩ ∈ DOMAIN CostLeq
    BY ⟨1⟩1, ⟨1⟩2 DEF CostLeq
⟨1⟩4. CostLeq[⟨A, B⟩] = (Cost[A] ≤ Cost[B])
    BY ⟨1⟩3 DEF CostLeq
⟨1⟩5. ∧ Cost[A] = Cardinality(A)
      ∧ Cost[B] = Cardinality(B)
    BY ⟨1⟩2, ⟨1⟩1
⟨1⟩ QED
    BY ⟨1⟩4, ⟨1⟩5


PROPOSITION MinCoverProperties ≜
    ASSUME
        NEW Leq, NEW C, NEW X, NEW Y,
        IsAMinCover(C, X, Y, Leq)
    PROVE
        ∧ C ∈ SUBSET Y
        ∧ IsACover(C, X, Leq)
        ∧ ∀ r ∈ SUBSET Y :   Any other cover from Y
            ∨ ¬ ∧ IsACover(r, X, Leq)
                ∧ CostLeq[⟨r, C⟩]
            ∨ CostLeq[⟨C, r⟩]   costs no less.
PROOF
⟨1⟩ DEFINE Covers ≜ CoversOf(X, Y, Leq)
⟨1⟩1. IsMinimal(C, Covers, CostLeq)
    BY DEF IsAMinCover
⟨1⟩2. C ∈ Covers
    BY ⟨1⟩1 DEF IsMinimal
⟨1⟩3. ∧ C ∈ SUBSET Y
      ∧ IsACover(C, X, Leq)
    BY ⟨1⟩2 DEF CoversOf
⟨1⟩ HIDE DEF CostLeq
```

⟨1⟩4. $\forall\, r \in \text{SUBSET}\ Y$:
$\lor \neg \land \mathit{IsACover}(r,\ X,\ \mathit{Leq})$
$\land\ \mathit{CostLeq}[\langle r,\ C\rangle]$
$\lor\ \mathit{CostLeq}[\langle C,\ r\rangle]$
BY ⟨1⟩1 DEF $\mathit{IsMinimal}$, $\mathit{CoversOf}$
⟨1⟩ QED
BY ⟨1⟩3, ⟨1⟩4

The previous proposition when we have Cardinality as Cost.
PROPOSITION $\mathit{MinCoverPropertiesCard} \triangleq$
ASSUME
NEW Leq, NEW Z, NEW C, NEW X,
NEW $Y \in \text{SUBSET}\ Z$,
$\land\ \mathit{IsAMinCover}(C,\ X,\ Y,\ \mathit{Leq})$
$\land\ \mathit{CardinalityAsCost}(Z)$
PROVE
$\land\ C \in \text{SUBSET}\ Y$
$\land\ \mathit{IsACover}(C,\ X,\ \mathit{Leq})$
$\land \forall\, r \in \text{SUBSET}\ Y$:
$\lor \neg \land \mathit{IsACover}(r,\ X,\ \mathit{Leq})$
$\land\ (\mathit{Cardinality}(r) \leq \mathit{Cardinality}(C))$
$\lor\ (\mathit{Cardinality}(C) \leq \mathit{Cardinality}(r))$
PROOF
⟨1⟩1. $\land\ C \in \text{SUBSET}\ Y$
$\land\ \mathit{IsACover}(C,\ X,\ \mathit{Leq})$
$\land \forall\, r \in \text{SUBSET}\ Y$:
$\lor \neg \land \mathit{IsACover}(r,\ X,\ \mathit{Leq})$
$\land\ \mathit{CostLeq}[\langle r,\ C\rangle]$
$\lor\ \mathit{CostLeq}[\langle C,\ r\rangle]$
⟨2⟩1. $\mathit{IsAMinCover}(C,\ X,\ Y,\ \mathit{Leq})$
OBVIOUS
⟨2⟩ QED
BY ⟨2⟩1, $\mathit{MinCoverProperties}$
⟨1⟩2. $Y \subseteq Z$
OBVIOUS
⟨1⟩3. $C \subseteq Z$
BY ⟨1⟩1, ⟨1⟩2
⟨1⟩4. ASSUME NEW $r \in \text{SUBSET}\ Y$
PROVE
$\land\ \mathit{CostLeq}[\langle r,\ C\rangle] = (\mathit{Cardinality}(r)\ \leq \mathit{Cardinality}(C))$
$\land\ \mathit{CostLeq}[\langle C,\ r\rangle] = (\mathit{Cardinality}(C) \leq \mathit{Cardinality}(r))$
⟨2⟩1. $r \in \text{SUBSET}\ Z$
BY ⟨1⟩4, ⟨1⟩2
⟨2⟩ QED

⟨3⟩1. $CardinalityAsCost(Z)$
OBVIOUS
⟨3⟩ QED
BY ⟨1⟩3, ⟨2⟩1, $CostLeqToCard$
⟨1⟩ QED
BY ⟨1⟩1, ⟨1⟩4

COROLLARY $MinCoverHasMinCard \triangleq$
ASSUME
NEW Leq, NEW Z, NEW C, NEW X,
NEW $Y \in$ SUBSET Z,
NEW $r \in$ SUBSET Y,
$\land\ CardinalityAsCost(Z)$
$\land\ Cardinality(C) \in Nat$
$\land\ Cardinality(r) \in Nat$
$\land\ IsAMinCover(C, X, Y, Leq)$
$\land\ IsACover(r, X, Leq)$
PROVE
$Cardinality(C) \leq Cardinality(r)$
PROOF
⟨1⟩1. $\lor\ Cardinality(C) \leq Cardinality(r)$
$\lor\ Cardinality(r) \leq Cardinality(C)$
OBVIOUS
⟨1⟩ QED
BY ⟨1⟩1, $MinCoverPropertiesCard$

Any two minimal covers C, H have the same cardinality, because X, Y are subsets of a finite complete lattice.

THEOREM $AllMinCoversSameCard \triangleq$
ASSUME
NEW C, NEW H, NEW Leq, NEW X, NEW Y, NEW Z,
$\land\ IsAMinCover(C, X, Y, Leq)$
$\land\ IsAMinCover(H, X, Y, Leq)$
$\land\ CardinalityAsCost(Z)$
$\land\ IsFiniteSet(Y)$
$\land\ Y \subseteq Z$
PROVE
$Cardinality(C) = Cardinality(H)$
PROOF
⟨1⟩1. $\land\ H \in$ SUBSET Y
$\land\ IsACover(H, X, Leq)$
$\land\ \forall\, r \in$ SUBSET Y :
$\lor\ \neg\ \land\ IsACover(r, X, Leq)$
$\land\ Cardinality(r) \leq Cardinality(H)$

$\lor$ $Cardinality(H) \leq Cardinality(r)$

$\langle 2 \rangle 1$. $IsAMinCover(H,\ X,\ Y,\ Leq)$

OBVIOUS

$\langle 2 \rangle$ QED

BY $\langle 2 \rangle 1$, $MinCoverPropertiesCard$

$\langle 1 \rangle 2$. $\land\ C \in$ SUBSET Y

$\land\ IsACover(C,\ X,\ Leq)$

$\land\ \forall\, r \in$ SUBSET Y :

$\lor\ \neg\ \land\ IsACover(r,\ X,\ Leq)$

$\land\ Cardinality(r) \leq Cardinality(C)$

$\lor\ Cardinality(C) \leq Cardinality(r)$

$\langle 2 \rangle 1$. $IsAMinCover(C,\ X,\ Y,\ Leq)$

OBVIOUS

$\langle 2 \rangle$ QED

BY $\langle 2 \rangle 1$, $MinCoverPropertiesCard$

$\langle 1 \rangle 3$. $(Cardinality(C) \leq Cardinality(H))$

$\Rightarrow (Cardinality(H) \leq Cardinality(C))$

BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$ $r \leftarrow C$ *in* $\langle 1 \rangle 1$

$\langle 1 \rangle 4$. $(Cardinality(H) \leq Cardinality(C))$

$\Rightarrow (Cardinality(C) \leq Cardinality(H))$

BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$ $r \leftarrow H$ *in* $\langle 1 \rangle 2$

$\langle 1 \rangle 5$. $\land\ Cardinality(C) \in Nat$

$\land\ Cardinality(H) \in Nat$

$\langle 2 \rangle 1$. $IsFiniteSet(C) \land IsFiniteSet(H)$

$\langle 3 \rangle 1$. $\land\ C \subseteq Y$

$\land\ H \subseteq Y$

$\langle 4 \rangle 1$. $\land\ IsAMinCover(C,\ X,\ Y,\ Leq)$

$\land\ IsAMinCover(H,\ X,\ Y,\ Leq)$

OBVIOUS

$\langle 4 \rangle$ QED

BY $\langle 4 \rangle 1$, $MinCoverProperties$

$\langle 3 \rangle 2$. $IsFiniteSet(Y)$

OBVIOUS

$\langle 3 \rangle$ QED

BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, FS_Subset

$\langle 2 \rangle$ QED

BY $\langle 2 \rangle 1$, $FS\_CardinalityType$

$\langle 1 \rangle 6$. CASE $Cardinality(C) \leq Cardinality(H)$

$\langle 2 \rangle 1$. $Cardinality(H) \leq Cardinality(C)$

BY $\langle 1 \rangle 6$, $\langle 1 \rangle 3$

$\langle 2 \rangle$ QED

BY $\langle 1 \rangle 6$, $\langle 2 \rangle 1$, $\langle 1 \rangle 5$

$\langle 1 \rangle 7$. ASSUME $\neg(Cardinality(C) \leq Cardinality(H))$

PROVE FALSE

$\langle 2 \rangle 1$. $Cardinality(C) > Cardinality(H)$

BY $\langle 1\rangle 7$, $\langle 1\rangle 5$

$\langle 2\rangle 2$. $Cardinality(C) \geq Cardinality(H)$

BY $\langle 2\rangle 1$, $\langle 1\rangle 5$

$\langle 2\rangle 3$. $Cardinality(C) \leq Cardinality(H)$

BY $\langle 2\rangle 2$, $\langle 1\rangle 4$

$\langle 2\rangle$ QED

BY $\langle 1\rangle 7$, $\langle 2\rangle 3$

$\langle 1\rangle$ QED

BY $\langle 1\rangle 6$, $\langle 1\rangle 7$

THEOREM $MinCoverEquivCoverCard \triangleq$

ASSUME

NEW Leq, NEW X, NEW Y, NEW Z,
NEW C, NEW H,
$\land IsAMinCover(C, X, Y, Leq)$
$\land IsFiniteSet(Y)$
$\land Y \subseteq Z$
$\land CardinalityAsCost(Z)$

PROVE

$IsAMinCover(H, X, Y, Leq)$
$\equiv \land H \in \text{SUBSET } Y$
$\land IsACover(H, X, Leq)$
$\land Cardinality(H) \leq Cardinality(C)$

PROOF

$\langle 1\rangle$ DEFINE

$Props \triangleq \land H \in \text{SUBSET } Y$
$\land IsACover(H, X, Leq)$
$\land Cardinality(H) \leq Cardinality(C)$

$Covers \triangleq CoversOf(X, Y, Leq)$

$\langle 1\rangle$ USE DEF $CoversOf$

$\langle 1\rangle 1$. ASSUME $IsAMinCover(H, X, Y, Leq)$
PROVE $Props$

$\langle 2\rangle 1$. $\land H \in \text{SUBSET } Y$
$\land IsACover(H, X, Leq)$
BY $\langle 1\rangle 1$, $MinCoverProperties$

$\langle 2\rangle 2$. $Cardinality(H) = Cardinality(C)$
BY $\langle 1\rangle 1$, $AllMinCoversSameCard$

$\langle 2\rangle 3$. $\land Cardinality(H) \in Nat$
$\land Cardinality(C) \in Nat$
BY $\langle 1\rangle 1$, $MinCoverProperties$, FS_Subset, $FS\_CardinalityType$

$\langle 2\rangle$ QED

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

$\langle 1\rangle 2$. ASSUME $Props$

PROVE $IsAMinCover(H,\ X,\ Y,\ Leq)$
⟨2⟩1. SUFFICES $IsMinimal(H,\ Covers,\ CostLeq)$
BY ⟨1⟩2 DEF $IsAMinCover$
⟨2⟩2. SUFFICES
ASSUME NEW $u \in Covers,\ CostLeq[\langle u,\ H\rangle]$
PROVE $CostLeq[\langle H,\ u\rangle]$
BY ⟨1⟩2, ⟨2⟩2 DEF $IsMinimal$
⟨2⟩7. $\wedge\ H \in \text{SUBSET } Z$
$\wedge\ u \in \text{SUBSET } Z$
BY ⟨1⟩2, ⟨2⟩2, $Y \subseteq Z$
⟨2⟩6. SUFFICES $Cardinality(H) \leq Cardinality(u)$
BY ⟨2⟩7, $CostLeqToCard$
⟨2⟩5. $\wedge\ Cardinality(H) \in Nat$
$\wedge\ Cardinality(C) \in Nat$
$\wedge\ Cardinality(u) \in Nat$
⟨3⟩1. $\wedge\ H \in \text{SUBSET } Y$
$\wedge\ C \in \text{SUBSET } Y$
$\wedge\ u \in \text{SUBSET } Y$
BY ⟨1⟩2, $MinCoverProperties$, ⟨2⟩2
⟨3⟩ QED
BY ⟨3⟩1, FS_Subset, $FS\_CardinalityType$
⟨2⟩4. $Cardinality(H) \leq Cardinality(C)$
BY ⟨1⟩2
⟨2⟩3. $Cardinality(C) \leq Cardinality(u)$
⟨3⟩1. $Cardinality(u) \leq Cardinality(H)$
BY ⟨2⟩2, ⟨2⟩5, ⟨2⟩7, $CostLeqToCard$
⟨3⟩2. $Cardinality(u) \leq Cardinality(C)$
BY ⟨2⟩4, ⟨3⟩1, ⟨2⟩5
⟨3⟩ QED
BY ⟨3⟩2, ⟨2⟩2, $MinCoverPropertiesCard$, ⟨2⟩5
⟨2⟩ QED
BY ⟨2⟩3, ⟨2⟩4, ⟨2⟩5
⟨1⟩ QED
BY ⟨1⟩1, ⟨1⟩2

PROPOSITION $CheaperCoverExists \triangleq$
ASSUME
NEW Leq, NEW X, NEW Y,
NEW $C \in CoversOf(X,\ Y,\ Leq)$, *so some cover exists*
$\neg IsAMinCover(C,\ X,\ Y,\ Leq)$
PROVE
$\exists\, OtherCover \in \text{SUBSET } Y :$
$\wedge\ OtherCover \neq C$
$\wedge\ IsACover(OtherCover,\ X,\ Leq)$

$\land$ $CostLeq[\langle OtherCover,\ C\rangle]$
$\land \neg CostLeq[\langle C,\ OtherCover\rangle]$
PROOF
BY $SmallerExists$ DEF $IsAMinCover$, $CoversOf$, $IsMinimal$

LEMMA $SubtractFromBoth \triangleq$
ASSUME
NEW Leq, NEW X, NEW E, NEW C,
LET
$Z \triangleq Support(Leq)$
IN
$\land\ IsAntiSymmetric(Leq)$
$\land\ E \subseteq X$
$\land\ X \subseteq Z$
$\land\ X = Maxima(X,\ Leq)$
$\land\ IsACover(C,\ X,\ Leq)$
PROVE
LET
$Xe \triangleq X \setminus E$
$Ce \triangleq C \setminus E$
IN
$IsACover(Ce,\ Xe,\ Leq)$
PROOF
$\langle 1\rangle$ DEFINE
$Xe \triangleq X \setminus E$
$Ce \triangleq C \setminus E$
$\langle 1\rangle 1$. SUFFICES ASSUME NEW $u \in Xe$
PROVE $\exists\, v \in Ce :\ Leq[u,\ v]$
BY DEF $IsACover$
$\langle 1\rangle 2$. PICK $v \in C :\ Leq[u,\ v]$
BY DEF $IsACover$
$\langle 1\rangle 3$. SUFFICES ASSUME $v \in E$
PROVE FALSE
BY $\langle 1\rangle 2$, $\langle 1\rangle 3$ DEF Ce
$\langle 1\rangle 4$. $u \neq v$
BY $\langle 1\rangle 1$, $\langle 1\rangle 3$ DEF Xe
$\langle 1\rangle$ QED
$\langle 2\rangle 1$. $IsAntiChain(X,\ Leq)$
BY $MaximaIsAntiChain$
$\langle 2\rangle 2$. $\land\ u \in X$
$\land\ v \in X$
BY $\langle 1\rangle 1$, $\langle 1\rangle 3$
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1$, $\langle 1\rangle 2$, $\langle 1\rangle 4$, $\langle 2\rangle 2$ DEF $IsAntiChain$

LEMMA $AddToBoth \triangleq$

ASSUME

NEW Leq, NEW X, NEW Y, NEW E, NEW C,

$\land\ C \subseteq Y$

$\land\ E \subseteq Support(Leq)$

$\land\ IsReflexive(Leq)$

$\land\ IsACoverFrom(C,\ X,\ Y,\ Leq)$

PROVE

LET

$XE \triangleq X \cup E$

$YE \triangleq Y \cup E$

$CE \triangleq C \cup E$

IN

$IsACoverFrom(CE,\ XE,\ YE,\ Leq)$

PROOF

⟨1⟩ DEFINE

$XE \triangleq X \cup E$

$YE \triangleq Y \cup E$

$CE \triangleq C \cup E$

⟨1⟩1. $IsACover(C,\ X,\ Leq)$

BY DEF $IsACoverFrom$

⟨1⟩2. $IsACover(CE,\ XE,\ Leq)$

⟨3⟩1. $\forall\, x \in X :\ \exists\, y \in C :\ Leq[x,\ y]$

BY ⟨1⟩1 DEF $IsACover$

⟨3⟩2. $\forall\, x \in XE :\ \exists\, y \in CE :\ Leq[x,\ y]$

BY ⟨3⟩1 DEF $IsReflexive$

⟨3⟩ QED

BY ⟨3⟩2 DEF $IsACover$

⟨1⟩3. $CE \in$ SUBSET YE

OBVIOUS

⟨1⟩ QED

BY ⟨1⟩2, ⟨1⟩3 DEF $IsACoverFrom$

(∗ *Proofs checked with TLAPS version* 1.4.3 ∗)

MODULE *Lattices*

Operations for minimal covering within a lattice, and theorems about them.

– bounds, Supremum, Infimum, sets of elements above and below
– Floor, Feil, Floors, Ceilings, MaxFloors, MaxCeilings
– quasiorder, partial order, lattice, complete lattice
– some reverse operations : Hat, MaxHat, unfloor
– properties of the above

The results from this module form the basis for proving correct the algorithm in the module CyclicCore.tla.

Author : Ioannis Filippidis

References

[1] *Olivier Coudert*
"Two-level logic minimization: An overview"
Integration, the VLSI Journal
*Vol.*17, *No.*2, *Oct* 1994, *pp.*97 −− 140
10.1016/0167 − 9260(94)00007 − 7

EXTENDS
FiniteSetFacts,
MinCover,
Optimization

$ThoseUnder(X,\ y,\ Leq) \triangleq \{x \in X :\ Leq[x,\ y]\}$
$ThoseOver(Y,\ x,\ Leq) \triangleq \{y \in Y :\ Leq[x,\ y]\}$
$Umbrella(x,\ X,\ Y,\ Leq) \triangleq$ UNION $\{$
$\quad ThoseUnder(X,\ y,\ Leq) :\ y \in ThoseOver(Y,\ x,\ Leq)\}$

$IsBelow(r,\ S,\ Leq) \triangleq \forall\, u \in S :\ Leq[r,\ u]$
$IsAbove(r,\ S,\ Leq) \triangleq \forall\, u \in S :\ Leq[u,\ r]$
$IsTightBound(r,\ S,\ Leq) \triangleq$
LET
$\quad Z \triangleq Support(Leq)$
IN
$\quad \wedge\, r \in Z$
$\quad \wedge\, IsAbove(r,\ S,\ Leq)$
$\quad \wedge \forall\, q \in Z :\ IsAbove(q,\ S,\ Leq) \Rightarrow Leq[r,\ q]$

$HasTightBound(S,\ Leq) \triangleq$
LET $Z \triangleq Support(Leq)$
IN $\exists\, r \in Z :\ IsTightBound(r,\ S,\ Leq)$

$$TightBound(S,\ Leq) \triangleq$$
$$\quad \text{LET } Z \triangleq Support(Leq)$$
$$\quad \text{IN } \quad \text{CHOOSE } r \in Z :\ IsTightBound(r,\ S,\ Leq)$$

$$UpsideDown(Leq) \triangleq$$
$$\quad \text{LET } Z \triangleq Support(Leq)$$
$$\quad \text{IN } \quad [t \in Z \times Z \mapsto Leq[t[2],\ t[1]]]$$

$$HasSup(S,\ Leq) \triangleq HasTightBound(S,\ Leq)$$
$$HasInf(S,\ Leq) \triangleq \text{LET } Geq \triangleq UpsideDown(Leq)$$
$$\qquad\qquad\qquad\qquad \text{IN } \quad HasTightBound(S,\ Geq)$$

$$Supremum(S,\ Leq) \triangleq TightBound(S,\ Leq)$$
$$Infimum(S,\ Leq) \triangleq \text{LET } Geq \triangleq UpsideDown(Leq)$$
$$\qquad\qquad\qquad\qquad \text{IN } \quad TightBound(S,\ Geq)$$

$$Floor(y,\ X,\ Leq) \triangleq Supremum(ThoseUnder(X,\ y,\ Leq),\ Leq)$$
$$Ceil(x,\ Y,\ Leq) \triangleq Infimum(ThoseOver(Y,\ x,\ Leq),\ Leq)$$

$$Floors(S,\ X,\ Leq) \triangleq \{Floor(y,\ X,\ Leq) :\ y \in S\}$$
$$Ceilings(S,\ Y,\ Leq) \triangleq \{Ceil(x,\ Y,\ Leq) :\ x \in S\}$$

In Coudert s terminology:

1. \max\tau_X or "column reduction" the operator *MaxFloors*
2.*\max\tau_Y or* "row reduction" *the operator MaxCeilings*

$$MaxFloors(S,\ X,\ Leq) \triangleq Maxima(Floors(S,\ X,\ Leq),\ Leq)$$
$$MaxCeilings(S,\ Y,\ Leq) \triangleq Maxima(Ceilings(S,\ Y,\ Leq),\ Leq)$$

$$IsAQuasiOrder(R) \triangleq \ \wedge IsReflexive(R) \ \wedge IsTransitive(R)$$
$$\qquad\qquad\qquad\qquad\quad \wedge IsAFunction(R) \wedge \exists S :\ S \times S = \text{DOMAIN } R$$

$$IsAPartialOrder(R) \triangleq$$
$$\quad \wedge IsReflexive(R) \ \wedge IsTransitive(R) \wedge IsAntiSymmetric(R)$$
$$\quad \wedge IsAFunction(R) \wedge \exists S :\ S \times S = \text{DOMAIN } R$$

$$IsALattice(R) \triangleq$$
$$\quad \wedge IsAPartialOrder(R)$$
$$\quad \wedge \text{LET } Z \triangleq Support(R)$$
$$\qquad \text{IN } \quad \forall S \in \text{SUBSET } Z :\ \vee Cardinality(S) \neq 2$$
$$\qquad\qquad\qquad\qquad\quad \vee HasInf(S,\ R) \wedge HasSup(S,\ R)$$

$$IsACompleteLattice(R) \triangleq$$
$$\quad \wedge IsAPartialOrder(R)$$
$$\quad \wedge \text{LET } Z \triangleq Support(R)$$
$$\qquad \text{IN } \quad \forall S \in \text{SUBSET } Z :\ HasInf(S,\ R) \wedge HasSup(S,\ R)$$

$$SomeAbove(u,\ Y,\ Leq) \triangleq \text{CHOOSE } r \in Y :\ Leq[u,\ r]$$
$$SomeMaxAbove(u,\ Y,\ Leq) = SomeAbove(u,\ Maxima(Y,\ Leq),\ Leq)$$

$SomeMaxAbove(u,\ Y,\ Leq) \triangleq \text{CHOOSE } m \in Maxima(Y,\ Leq) :\ Leq[u,\ m]$
$Hat(S,\ Y,\ Leq) \triangleq \{SomeAbove(y,\ Y,\ Leq) :\ y \in S\}$
$IsAHat(H,\ C,\ Y,\ Leq) \triangleq$
$\quad \land H \in \text{SUBSET } Y$
$\quad \land Refines(C,\ H,\ Leq)$
$\quad \land Cardinality(H) \leq Cardinality(C)$
$MaxHat(S,\ Y,\ Leq) = Hat(S,\ Maxima(Y,\ Leq),\ Leq)$
$MaxHat(S,\ Y,\ Leq) \triangleq \{SomeMaxAbove(y,\ Y,\ Leq) :\ y \in S\}$

$SomeUnfloor(u,\ X,\ Y,\ Leq) \triangleq \text{CHOOSE } y \in Y :\ u = Floor(y,\ X,\ Leq)$
$Unfloors(S,\ X,\ Y,\ Leq) \triangleq \{SomeUnfloor(y,\ X,\ Y,\ Leq) :\ y \in S\}$

Unfloors satisfies IsUnfloor, but we use IsUnfloor to prove theorems in order to be able to replace Unfloors with the more concrete and computationally simpler Hat when F is an antichain.

$IsUnfloor(C,\ F,\ X,\ Leq) \triangleq \land F = Floors(C,\ X,\ Leq)$
$\qquad\qquad\qquad\qquad\quad \land Cardinality(C) \leq Cardinality(F)$

Properties of lattices.

THEOREM $LatticeProperties \triangleq$
ASSUME
NEW Leq, $IsACompleteLattice(Leq)$
PROVE
$\land IsReflexive(Leq)$
$\land IsTransitive(Leq)$
$\land IsAntiSymmetric(Leq)$
$\land IsAFunction(Leq)$
$\land \exists S :\ S \times S = \text{DOMAIN } Leq$
$\land \text{LET } Z \triangleq Support(Leq)$
IN $\forall S \in \text{SUBSET } Z :\ HasInf(S,\ Leq) \land HasSup(S,\ Leq)$
PROOF
BY DEF $IsACompleteLattice$, $IsAPartialOrder$

THEOREM $SupIsUnique \triangleq$
ASSUME
NEW Leq, NEW S,
$S \subseteq Support(Leq)$,
$IsACompleteLattice(Leq)$
PROVE
LET $Z \triangleq Support(Leq)$
IN $\forall u,\ v \in Z :$
$(IsTightBound(u,\ S,\ Leq) \land IsTightBound(v,\ S,\ Leq))$
$\Rightarrow (u = v)$
PROOF

BY DEF $IsTightBound$, $IsACompleteLattice$, $IsAPartialOrder$, $IsAntiSymmetric$

THEOREM $SupExists \triangleq$
ASSUME
NEW Leq, NEW S,
$\land IsACompleteLattice(Leq)$
$\land S \subseteq Support(Leq)$
PROVE
LET
$Z \triangleq Support(Leq)$
$r \triangleq Supremum(S, Leq)$
IN
$\land r \in Z$
$\land IsAbove(r, S, Leq)$
$\land \forall q \in Z : IsAbove(q, S, Leq) \Rightarrow Leq[r, q]$
PROOF
BY DEF $IsACompleteLattice$, $Supremum$, $HasSup$, $HasTightBound$, $TightBound$, $IsTightBound$

THEOREM $InfExists \triangleq$
ASSUME
NEW Leq, NEW S,
$IsACompleteLattice(Leq)$,
$S \subseteq Support(Leq)$
PROVE
LET
$Z \triangleq Support(Leq)$
$r \triangleq Infimum(S, Leq)$
IN
$\land r \in Z$
$\land IsBelow(r, S, Leq)$
$\land \forall q \in Z : IsBelow(q, S, Leq) \Rightarrow Leq[q, r]$
PROOF OMITTED

THEOREM $SupIsMonotonic \triangleq$
ASSUME
NEW Leq, NEW A, NEW B,
$IsACompleteLattice(Leq)$,
LET $Z \triangleq Support(Leq)$
IN $\land A \subseteq B$
$\land B \subseteq Z$
PROVE
LET
$a \triangleq Supremum(A, Leq)$

```
        b ≜ Supremum(B, Leq)
    IN
        Leq[a, b]
PROOF OMITTED

THEOREM SupOfRefinement ≜
    ASSUME
        NEW Leq, NEW A, NEW B,
        IsACompleteLattice(Leq),
        LET Z ≜ Support(Leq)
        IN   ∧ A ⊆ Z
             ∧ B ⊆ Z,
        ∀ u ∈ A : ∃ v ∈ B : Leq[u, v]
    PROVE
        LET
            a ≜ Supremum(A, Leq)
            b ≜ Supremum(B, Leq)
        IN
            Leq[a, b]
    PROOF
    ⟨1⟩ DEFINE
        Z ≜ Support(Leq)
        a ≜ Supremum(A, Leq)
        b ≜ Supremum(B, Leq)
    ⟨1⟩2. ∧ a ∈ Z
          ∧ IsAbove(a, A, Leq)
          ∧ ∀ q ∈ Z : IsAbove(q, A, Leq) ⇒ Leq[a, q]
        BY SupExists
    ⟨1⟩3. ∧ b ∈ Z
          ∧ IsAbove(b, B, Leq)
          ∧ ∀ q ∈ Z : IsAbove(q, B, Leq) ⇒ Leq[b, q]
        BY SupExists
    ⟨1⟩4. IsAbove(b, A, Leq)
        ⟨2⟩1. SUFFICES ASSUME NEW u ∈ A
                       PROVE Leq[u, b]
            BY DEF IsAbove
        ⟨2⟩ DEFINE v ≜ CHOOSE r ∈ B : Leq[u, r]
        ⟨2⟩2. Leq[u, v]
            OBVIOUS
        ⟨2⟩3. Leq[v, b]
            BY ⟨1⟩3 DEF IsAbove
        ⟨2⟩ QED
            ⟨3⟩1. IsTransitive(Leq)
                BY DEF IsACompleteLattice, IsAPartialOrder
```

```
        ⟨3⟩2. (u ∈ Z) ∧ (v ∈ Z) ∧ (b ∈ Z)
            BY ⟨1⟩3
        ⟨3⟩ QED
            BY ⟨2⟩2, ⟨2⟩3, ⟨3⟩1, ⟨3⟩2  DEF IsTransitive
    ⟨1⟩ QED
        BY ⟨1⟩2, ⟨1⟩3, ⟨1⟩4

LEMMA PartialOrderHasSymmetricDomain ≜
    ASSUME
        NEW Leq,
        IsAPartialOrder(Leq)
    PROVE
        LET Z ≜ Support(Leq)
        IN  (DOMAIN Leq) = (Z × Z)
    PROOF
    ⟨1⟩ DEFINE Z ≜ Support(Leq)
    ⟨1⟩1. PICK S : (DOMAIN Leq) = (S × S)
        BY  DEF IsAPartialOrder
    ⟨1⟩2. SUFFICES Z = S
        BY ⟨1⟩1
    ⟨1⟩3. Z ⊆ S
        BY ⟨1⟩1  DEF Support
    ⟨1⟩4. S ⊆ Z
        ⟨3⟩ SUFFICES ASSUME NEW u ∈ S
                     PROVE u ∈ Z
            OBVIOUS
        ⟨3⟩ QED
            BY ⟨1⟩1  DEF Support
    ⟨1⟩ QED
        BY ⟨1⟩3, ⟨1⟩4

COROLLARY LatticeHasSymmetricDomain ≜
    ASSUME
        NEW Leq,
        IsACompleteLattice(Leq)
    PROVE
        LET Z ≜ Support(Leq)
        IN  (DOMAIN Leq) = (Z × Z)
    PROOF
    BY PartialOrderHasSymmetricDomain DEF IsACompleteLattice
```

Properties of Floor

```
SupExists for Floor
PROPOSITION FloorExists ≜
  ASSUME
    NEW Leq, NEW X, NEW y,
    LET
      Z ≜ Support(Leq)
    IN
      ∧ IsACompleteLattice(Leq)
      ∧ X ⊆ Z
  PROVE
    LET
      Z ≜ Support(Leq)
      U ≜ ThoseUnder(X, y, Leq)
      f ≜ Floor(y, X, Leq)
    IN
      ∧ f ∈ Z
      ∧ IsAbove(f, U, Leq)
      ∧ ∀ q ∈ Z : IsAbove(q, U, Leq) ⇒ Leq[f, q]
  PROOF
  ⟨1⟩ DEFINE
      Z ≜ Support(Leq)
      U ≜ ThoseUnder(X, y, Leq)
      f ≜ Floor(y, X, Leq)
  ⟨1⟩1. U ⊆ Z
      BY DEF ThoseUnder
  ⟨1⟩2. f = Supremum(U, Leq)
      BY DEF Floor
  ⟨1⟩ QED
      BY ⟨1⟩1, ⟨1⟩2, SupExists

COROLLARY FloorsIsSubset ≜
  ASSUME
    NEW Leq, NEW X, NEW S,
    LET
      Z ≜ Support(Leq)
    IN
      ∧ X ⊆ Z
      ∧ S ⊆ Z
      ∧ IsACompleteLattice(Leq)
  PROVE
    LET Z ≜ Support(Leq)
    IN  Floors(S, X, Leq) ⊆ Z
  PROOF
  BY FloorExists DEF Floors
```

```
(* If u is below y, then u is below Floor(y, X, Leq) *)
PROPOSITION FloorIsAboveThoseUnder ≜
  ASSUME
    NEW Leq, NEW X, NEW Y, NEW y, NEW u ∈ X,
    LET
      Z ≜ Support(Leq)
    IN
      ∧ X ⊆ Z
      ∧ IsACompleteLattice(Leq)
      ∧ Leq[u, y]
  PROVE
    LET fy ≜ Floor(y, X, Leq)
    IN  Leq[u, fy]
  PROOF
  ⟨1⟩ DEFINE
      U ≜ ThoseUnder(X, y, Leq)
      fy ≜ Floor(y, X, Leq)
  ⟨1⟩1. u ∈ U
      BY DEF ThoseUnder
  ⟨1⟩2. U ⊆ X
      BY DEF ThoseUnder
  ⟨1⟩3. fy = Supremum(U, Leq)
      BY DEF Floor
  ⟨1⟩ QED
      BY ⟨1⟩1, ⟨1⟩2, ⟨1⟩3, SupExists DEF IsAbove

THEOREM FloorIsMonotonic ≜
  ASSUME
    NEW Leq, NEW X, NEW u, NEW v,
    IsACompleteLattice(Leq),
    LET
      Z ≜ Support(Leq)
    IN
      ∧ u ∈ Z
      ∧ v ∈ Z
      ∧ Leq[u, v]
      ∧ X ⊆ Z
  PROVE
    LET
      a ≜ Floor(u, X, Leq)
      b ≜ Floor(v, X, Leq)
    IN
      Leq[a, b]
  PROOF
```

⟨1⟩ DEFINE
$Z \triangleq Support(Leq)$
$A \triangleq ThoseUnder(X,\ u,\ Leq)$
$B \triangleq ThoseUnder(X,\ v,\ Leq)$
$a \triangleq Floor(u,\ X,\ Leq)$
$b \triangleq Floor(v,\ X,\ Leq)$
⟨1⟩2. $\wedge\ a = Supremum(A,\ Leq)$
$\wedge\ b = Supremum(B,\ Leq)$
BY DEF $Floor$
⟨1⟩3. $A \subseteq B$
BY $LatticeProperties$ DEF $IsTransitive,\ ThoseUnder$
⟨1⟩4. $B \subseteq Z$
⟨2⟩1. $B \subseteq X$
BY DEF $ThoseUnder$
⟨2⟩ QED
BY ⟨2⟩1
⟨1⟩ QED
BY ⟨1⟩2, ⟨1⟩3, ⟨1⟩4, $SupIsMonotonic$

THEOREM $FloorIsSmaller \triangleq$
ASSUME
NEW Leq, NEW X, NEW y,
$IsACompleteLattice(Leq)$,
LET $Z \triangleq Support(Leq)$
IN $\wedge\ y \in Z$
$\wedge\ X \subseteq Z$
PROVE
LET $r \triangleq Floor(y,\ X,\ Leq)$
IN $Leq[r,\ y]$
PROOF
⟨1⟩ DEFINE
$Z \triangleq Support(Leq)$
$r \triangleq Floor(y,\ X,\ Leq)$
$S \triangleq ThoseUnder(X,\ y,\ Leq)$
⟨1⟩2. $r = Supremum(S,\ Leq)$
BY DEF $Floor$
⟨1⟩3. $\forall\ q \in Z :\ IsAbove(q,\ S,\ Leq) \Rightarrow Leq[r,\ q]$
⟨2⟩1. $HasSup(S,\ Leq)$
BY DEF $IsACompleteLattice,\ ThoseUnder$
⟨2⟩2. $\exists\ u \in Z :\ IsTightBound(u,\ S,\ Leq)$
BY ⟨2⟩1 DEF $HasSup,\ HasTightBound$
⟨2⟩ QED
BY ⟨1⟩2, ⟨2⟩2 DEF $Supremum,\ TightBound,\ IsTightBound$
⟨1⟩4. $IsAbove(y,\ S,\ Leq)$

BY DEF $ThoseUnder$, $IsAbove$

$\langle 1 \rangle$ QED

BY $\langle 1 \rangle 3$, $\langle 1 \rangle 4$

PROPOSITION $FloorIsIdempotent \triangleq$

ASSUME

NEW Leq, NEW X, NEW v,

LET

$Z \triangleq Support(Leq)$

IN

$\land IsACompleteLattice(Leq)$

$\land X \subseteq Z$

$\land v \in Z$

$\land \exists\, y \in Z : \; v = Floor(y,\, X,\, Leq)$

PROVE

$v = Floor(v,\, X,\, Leq)$

PROOF

$\langle 1 \rangle$ DEFINE

$Z \triangleq Support(Leq)$

$\langle 1 \rangle 1$. PICK $y \in Z : \; v = Floor(y,\, X,\, Leq)$

OBVIOUS

$\langle 1 \rangle$ DEFINE

$Bv \triangleq ThoseUnder(X,\, v,\, Leq)$

$By \triangleq ThoseUnder(X,\, y,\, Leq)$

$fv \triangleq Floor(v,\, X,\, Leq)$

$fy \triangleq Floor(y,\, X,\, Leq)$

$\langle 1 \rangle 2$. $\land fv = Supremum(Bv,\, Leq)$

$\land fy = Supremum(By,\, Leq)$

BY DEF $Floor$

$\langle 1 \rangle 3$. $v = fy$

BY $\langle 1 \rangle 1$

$\langle 1 \rangle 4$. SUFFICES $fv = fy$

BY $\langle 1 \rangle 3$

$\langle 1 \rangle 5$. SUFFICES $Bv = By$

BY $\langle 1 \rangle 2$

$\langle 1 \rangle 6$. $By \subseteq Bv$

BY $\langle 1 \rangle 3$, $FloorIsAboveThoseUnder$ DEF $ThoseUnder$

$\langle 1 \rangle 7$. $Bv \subseteq By$

$\langle 2 \rangle 1$. SUFFICES ASSUME NEW $u \in Bv$

PROVE $u \in By$

OBVIOUS

$\langle 2 \rangle 2$. $Leq[u,\, v]$

BY $\langle 2 \rangle 1$ DEF $ThoseUnder$

$\langle 2 \rangle 3$. $Leq[v,\, y]$

```
            BY ⟨1⟩3, FloorIsSmaller
        ⟨2⟩4. Leq[u, y]
            ⟨3⟩1. IsTransitive(Leq)
                BY LatticeProperties
            ⟨3⟩2. u ∈ Z ∧ v ∈ Z ∧ y ∈ Z
                ⟨4⟩1. Bv ⊆ Z
                    BY DEF ThoseUnder
                ⟨4⟩2. u ∈ Z
                    BY ⟨2⟩1, ⟨4⟩1
                ⟨4⟩ QED
                    BY ⟨4⟩2, ⟨1⟩1
            ⟨3⟩3. Leq[u, v] ∧ Leq[v, y]
                BY ⟨2⟩2, ⟨2⟩3
            ⟨3⟩ QED
                BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3 DEF IsTransitive
        ⟨2⟩ QED
            BY ⟨2⟩4 DEF ThoseUnder
    ⟨1⟩ QED
        BY ⟨1⟩6, ⟨1⟩7

THEOREM FloorsSmaller ≜
    ASSUME
        NEW X, NEW Y, NEW Leq,
        IsFiniteSet(Y)
    PROVE
        LET
            R ≜ Floors(Y, X, Leq)
        IN
            ∧ IsFiniteSet(R)
            ∧ Cardinality(R) ≤ Cardinality(Y)
    PROOF
    BY ImageOfFinite DEF Floors

THEOREM MaxFloorSmaller ≜
    ASSUME
        NEW X, NEW Y, NEW Leq,
        IsFiniteSet(Y)
    PROVE
        LET
            R ≜ MaxFloors(Y, X, Leq)
            T ≜ Floors(Y, X, Leq)
        IN
            ∧ R ⊆ T
            ∧ IsFiniteSet(R) ∧ IsFiniteSet(T)
```

$\land\ Cardinality(R) \leq Cardinality(T)$
$\land\ Cardinality(T) \leq Cardinality(Y)$

PROOF

$\langle 1\rangle$ DEFINE
$R \triangleq MaxFloors(Y, X, Leq)$
$T \triangleq Floors(Y, X, Leq)$

$\langle 1\rangle 1.\ R = Maxima(T, Leq)$
BY DEF *MaxFloors*

$\langle 1\rangle 2.\ R \subseteq T$
BY $\langle 1\rangle 1$, *MaxIsSubset*

$\langle 1\rangle 3.\ \land\ IsFiniteSet(T)$
$\land\ Cardinality(T) \leq Cardinality(Y)$
BY *ImageOfFinite* DEF *Floors*

$\langle 1\rangle 4.\ \land\ IsFiniteSet(R)$
$\land\ Cardinality(R) \leq Cardinality(T)$
BY $\langle 1\rangle 2$, $\langle 1\rangle 3$, *FS_Subset*

$\langle 1\rangle$ QED
BY $\langle 1\rangle 2$, $\langle 1\rangle 3$, $\langle 1\rangle 4$, *FS_CardinalityType*

Geq properties.

THEOREM *UpsideDownHasSameSupport* $\triangleq$
ASSUME
NEW *Leq*
PROVE
LET
$Geq \triangleq UpsideDown(Leq)$
IN $Support(Geq) = Support(Leq)$

PROOF

$\langle 1\rangle$ DEFINE
$Z \triangleq Support(Leq)$
$Geq \triangleq UpsideDown(Leq)$

$\langle 1\rangle 1.\ Geq = [t \in Z \times Z \mapsto Leq[t[2],\ t[1]]]$
BY DEF *UpsideDown*

$\langle 1\rangle 2.\ Support(Geq) \subseteq Z$
$\langle 2\rangle 1.$ DOMAIN $Geq = Z \times Z$
BY $\langle 1\rangle 1$
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1$ DEF *Support*

$\langle 1\rangle 3.\ Z \subseteq Support(Geq)$
$\langle 3\rangle 1.\ \forall\, u \in Z :\ \exists\, p \in$ DOMAIN $Geq :\ p[1] = u$
BY $\langle 1\rangle 1$
$\langle 3\rangle 2.\ Z \subseteq \{p[1] :\ p \in$ DOMAIN $Geq\}$
BY $\langle 3\rangle 1$

```
        ⟨3⟩ QED
            BY ⟨3⟩2  DEF Support
    ⟨1⟩ QED
        BY ⟨1⟩2, ⟨1⟩3

LEMMA LeqSwapOfGeq ≜
    ASSUME
        NEW Leq
    PROVE
        LET
            Geq ≜ UpsideDown(Leq)
            Z ≜ Support(Leq)
            W ≜ Support(Geq)
        IN
            ∧ W = Z
            ∧ ∀ u, v ∈ W :  Geq[u, v] = Leq[v, u]
    PROOF
    ⟨1⟩ DEFINE
        Geq ≜ UpsideDown(Leq)
        Z ≜ Support(Leq)
        W ≜ Support(Geq)
    ⟨1⟩ W = Z
        BY UpsideDownHasSameSupport
    ⟨1⟩ SUFFICES ASSUME NEW u ∈ W, NEW v ∈ W
                 PROVE Geq[u, v] = Leq[v, u]
        OBVIOUS
    ⟨1⟩1. ⟨u, v⟩ ∈ Z × Z
        OBVIOUS
    ⟨1⟩ QED
        BY ⟨1⟩1  DEF UpsideDown

THEOREM SwapPreservesOrderProperties ≜
    ASSUME
        NEW Leq
    PROVE
        LET
            Z ≜ Support(Leq)
            Geq ≜ UpsideDown(Leq)
        IN
            ∧ IsReflexive(Leq) ⇒ IsReflexive(Geq)
            ∧ IsTransitive(Leq) ⇒ IsTransitive(Geq)
            ∧ IsAntiSymmetric(Leq) ⇒ IsAntiSymmetric(Geq)
    PROOF
    ⟨1⟩ DEFINE
```

$Z \triangleq Support(Leq)$
$Geq \triangleq UpsideDown(Leq)$
$W \triangleq Support(Geq)$
⟨1⟩1. $Geq = [t \in Z \times Z \mapsto Leq[t[2],\ t[1]]]$
BY DEF *UpsideDown*
⟨1⟩2. $W = Z$
BY *UpsideDownHasSameSupport*
⟨1⟩3. ASSUME *IsReflexive*(*Leq*)
PROVE *IsReflexive*(*Geq*)
⟨2⟩1. SUFFICES ASSUME NEW $x \in W$
PROVE $Geq[x,\ x]$
BY DEF *IsReflexive*
⟨2⟩2. $x \in Z$
BY ⟨1⟩2
⟨2⟩3. $Leq[x,\ x]$
BY ⟨1⟩3, ⟨2⟩2 DEF *IsReflexive*
⟨2⟩4. $\langle x,\ x\rangle \in Z \times Z$
BY ⟨2⟩2
⟨2⟩5. $Geq[\langle x,\ x\rangle] = Leq[\langle x,\ x\rangle]$
BY ⟨1⟩1, ⟨2⟩4
⟨2⟩ QED
BY ⟨2⟩3, ⟨2⟩5
⟨1⟩4. ASSUME *IsTransitive*(*Leq*)
PROVE *IsTransitive*(*Geq*)
⟨2⟩1. $\forall\, x,\ y,\ z \in Z :\ (Leq[x,\ y] \land Leq[y,\ z]) \Rightarrow Leq[x,\ z]$
BY ⟨1⟩4 DEF *IsTransitive*
⟨2⟩2. $\forall\, x,\ y,\ z \in Z :\ (Geq[y,\ x] \land Geq[z,\ y]) \Rightarrow Geq[z,\ x]$
BY ⟨2⟩1, ⟨1⟩1
⟨2⟩ QED
BY ⟨1⟩2, ⟨2⟩2 DEF *IsTransitive*
⟨1⟩5. ASSUME *IsAntiSymmetric*(*Leq*)
PROVE *IsAntiSymmetric*(*Geq*)
⟨2⟩1. SUFFICES ASSUME NEW $x \in W$, NEW $y \in W$,
$Geq[x,\ y] \land (x \neq y)$
PROVE $\neg Geq[y,\ x]$
BY DEF *IsAntiSymmetric*
⟨2⟩2. $x \in Z \land y \in Z$
BY ⟨2⟩1, ⟨1⟩2
⟨2⟩3. $\langle x,\ y\rangle \in Z \times Z$
BY ⟨2⟩2
⟨2⟩4. $Leq[y,\ x]$
BY ⟨2⟩1, ⟨1⟩1, ⟨2⟩3
⟨2⟩5. $\neg Leq[x,\ y]$
BY ⟨2⟩4, ⟨1⟩5, ⟨2⟩2, ⟨2⟩1 DEF *IsAntiSymmetric*
⟨2⟩ QED

```
            ⟨3⟩1. ⟨y, x⟩ ∈ Z × Z
                BY ⟨2⟩2
            ⟨3⟩ QED
                BY ⟨1⟩1, ⟨3⟩1, ⟨2⟩5
    ⟨1⟩ QED
        BY ⟨1⟩3, ⟨1⟩4, ⟨1⟩5

THEOREM UpsideDownIsLattice ≜
    ASSUME
        NEW Leq,
        IsACompleteLattice(Leq)
    PROVE
        LET Geq ≜ UpsideDown(Leq)
        IN  IsACompleteLattice(Geq)
    PROOF
    ⟨1⟩ DEFINE
        Z ≜ Support(Leq)
        Geq ≜ UpsideDown(Leq)
        W ≜ Support(Geq)
    ⟨1⟩1. Geq = [t ∈ Z × Z ↦ Leq[t[2], t[1]]]
        BY DEF UpsideDown
    ⟨1⟩2. Support(Geq) = Z
        BY UpsideDownHasSameSupport
    ⟨1⟩3. DOMAIN Leq = Z × Z
        BY LatticeHasSymmetricDomain
    ⟨1⟩4. IsReflexive(Geq) ∧ IsTransitive(Geq) ∧ IsAntiSymmetric(Geq)
        ⟨2⟩1. IsReflexive(Leq) ∧ IsTransitive(Leq) ∧ IsAntiSymmetric(Leq)
            BY DEF IsACompleteLattice, IsAPartialOrder
        ⟨2⟩ QED
            BY ⟨2⟩1, SwapPreservesOrderProperties
    ⟨1⟩5. IsAPartialOrder(Geq)
        ⟨2⟩1. IsAFunction(Geq)
            BY ⟨1⟩1 DEF IsAFunction
        ⟨2⟩2. DOMAIN Geq = Z × Z
            BY ⟨1⟩1
        ⟨2⟩ QED
            BY ⟨2⟩1, ⟨2⟩2, ⟨1⟩4 DEF IsAPartialOrder
    ⟨1⟩6. ASSUME NEW S ∈ SUBSET Z
          PROVE HasInf(S, Geq) ∧ HasSup(S, Geq)
        ⟨2⟩1. HasSup(S, Geq)
            ⟨3⟩1. HasInf(S, Leq)
                BY DEF IsACompleteLattice
            ⟨3⟩ QED
                BY ⟨3⟩1 DEF HasInf, HasSup
```

⟨2⟩2. $HasInf(S,\ Geq)$
⟨3⟩1. $HasSup(S,\ Leq)$
BY DEF $IsACompleteLattice$
⟨3⟩2. $Leq = UpsideDown(Geq)$
⟨4⟩1. $IsAFunction(Leq)$
BY DEF $IsACompleteLattice$, $IsAPartialOrder$
⟨4⟩2. $UpsideDown(Geq) = [t \in Z \times Z \mapsto Geq[t[2],\ t[1]]]$
BY ⟨1⟩2 DEF $UpsideDown$
⟨4⟩3. $\forall\, t \in Z \times Z :\ \ Geq[t[2],\ t[1]] = Leq[t[1],\ t[2]]$
⟨5⟩ HIDE DEF Geq
⟨5⟩ SUFFICES ASSUME NEW $t \in Z \times Z$
PROVE $Geq[t[2],\ t[1]] = Leq[t[1],\ t[2]]$
OBVIOUS
⟨5⟩1. $\langle t[2],\ t[1]\rangle \in Z \times Z$
OBVIOUS
⟨5⟩ QED
BY ⟨5⟩1, ⟨1⟩1
⟨4⟩4. $UpsideDown(Geq) = [t \in Z \times Z \mapsto Leq[t[1],\ t[2]]]$
BY ⟨4⟩3, ⟨4⟩2
⟨4⟩5. $UpsideDown(Geq) = [t \in Z \times Z \mapsto Leq[t]]$
BY ⟨4⟩4
⟨4⟩6. $Leq = [t \in Z \times Z \mapsto Leq[t]]$
BY ⟨1⟩3, ⟨4⟩1 DEF $IsAFunction$
⟨4⟩ QED
BY ⟨4⟩5, ⟨4⟩6
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2 DEF $HasSup$, $HasInf$
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2
⟨1⟩ QED
BY ⟨1⟩2, ⟨1⟩5, ⟨1⟩6 DEF $IsACompleteLattice$

Ceil properties.

PROPOSITION $CeilExists \triangleq$
ASSUME
NEW Leq, NEW Y, NEW x,
LET
$Z \triangleq Support(Leq)$
IN
$\land\ IsACompleteLattice(Leq)$
$\land\ Y \subseteq Z$
PROVE
LET

$Z \triangleq Support(Leq)$
$V \triangleq ThoseOver(Y,\ x,\ Leq)$
$c \triangleq Ceil(x,\ Y,\ Leq)$
IN
$\land\ c \in Z$
$\land\ IsBelow(c,\ V,\ Leq)$
$\land\ \forall\ q \in Z :\ IsBelow(q,\ V,\ Leq) \Rightarrow Leq[c,\ q]$
PROOF OMITTED *For symmetric reasons as FloorExists.*

COROLLARY $CeilingsIsSubset \triangleq$
ASSUME
NEW Leq, NEW Y, NEW S,
LET
$Z \triangleq Support(Leq)$
IN
$\land\ Y \subseteq Z$
$\land\ S \subseteq Z$
$\land\ IsACompleteLattice(Leq)$
PROVE
LET $Z \triangleq Support(Leq)$
IN $Ceilings(S,\ Y,\ Leq) \subseteq Z$
PROOF
BY $CeilExists$ DEF $Ceilings$

PROPOSITION $CeilIsBelowThoseOver \triangleq$
ASSUME
NEW Leq, NEW X, NEW Y, NEW x, NEW $v \in Y$,
LET
$Z \triangleq Support(Leq)$
IN
$\land\ Y \subseteq Z$
$\land\ IsACompleteLattice(Leq)$
$\land\ Leq[x,\ v]$
PROVE
LET $C \triangleq Ceil(x,\ Y,\ Leq)$
IN $Leq[C,\ v]$
PROOF
$\langle 1 \rangle$ DEFINE
$T \triangleq ThoseOver(Y,\ x,\ Leq)$
$C \triangleq Ceil(x,\ Y,\ Leq)$
$\langle 1 \rangle 1.\ v \in T$
BY DEF $ThoseOver$
$\langle 1 \rangle 2.\ T \subseteq Y$
BY DEF $ThoseOver$

⟨1⟩3. $C = Infimum(T,\ Leq)$
BY DEF $Ceil$
⟨1⟩ QED
BY ⟨1⟩1, ⟨1⟩2, ⟨1⟩3, $InfExists$ DEF $IsBelow$

THEOREM $CeilIsLarger \triangleq$
ASSUME
NEW Leq, NEW Y, NEW x,
$IsACompleteLattice(Leq)$,
LET $Z \triangleq Support(Leq)$
IN $\land x \in Z$
$\land Y \subseteq Z$
PROVE
LET $r \triangleq Ceil(x,\ Y,\ Leq)$
IN $Leq[x,\ r]$
PROOF
⟨1⟩ DEFINE
$Z \triangleq Support(Leq)$
$r \triangleq Ceil(x,\ Y,\ Leq)$
$Geq \triangleq UpsideDown(Leq)$
$S \triangleq ThoseUnder(Y,\ x,\ Geq)$
$w \triangleq Floor(x,\ Y,\ Geq)$
$P \triangleq Support(Geq)$
⟨1⟩1. $IsACompleteLattice(Geq)$
BY $UpsideDownIsLattice$
⟨1⟩2. $Geq = [t \in Z \times Z \mapsto Leq[t[2],\ t[1]]]$
BY DEF $UpsideDown$
⟨1⟩3. $Leq[x,\ w] = Geq[w,\ x]$
⟨2⟩1. $Z = P$
BY $UpsideDownHasSameSupport$
⟨2⟩2. $x \in Z$
OBVIOUS
⟨2⟩3. $w \in P$
⟨3⟩1. $w = Supremum(S,\ Geq)$
BY DEF $Floor$, $ThoseUnder$
⟨3⟩2. $S \subseteq Z$
BY DEF $ThoseUnder$
⟨3⟩3. $S \subseteq P$
BY ⟨2⟩1, ⟨3⟩2
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩3, ⟨1⟩1, $SupExists$
⟨2⟩4. DOMAIN $Leq = Z \times Z$
BY $LatticeHasSymmetricDomain$
⟨2⟩5. DOMAIN $Geq = Z \times Z$

BY $\langle 1 \rangle 2$
$\langle 2 \rangle 6$. $\langle x, w \rangle \in$ DOMAIN Leq
$\langle 3 \rangle$ HIDE DEF Z, P
$\langle 3 \rangle$ QED
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, $\langle 2 \rangle 3$, $\langle 2 \rangle 4$
$\langle 2 \rangle 7$. $\langle w, x \rangle \in$ DOMAIN Geq
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, $\langle 2 \rangle 3$, $\langle 2 \rangle 5$
$\langle 2 \rangle$ QED
BY $\langle 1 \rangle 2$, $\langle 2 \rangle 6$, $\langle 2 \rangle 7$
$\langle 1 \rangle 4$. $Leq[x, w]$
$\langle 2 \rangle 1$. $Z = Support(Geq)$
BY *UpsideDownHasSameSupport*
$\langle 2 \rangle 2$. $Geq[w, x]$
BY $\langle 1 \rangle 1$, $\langle 2 \rangle 1$, *FloorIsSmaller*
$\langle 2 \rangle$ QED
BY $\langle 2 \rangle 2$, $\langle 1 \rangle 3$
$\langle 1 \rangle 5$. $r = w$
$\langle 2 \rangle 1$. $ThoseOver(Y, x, Leq) = ThoseUnder(Y, x, Geq)$
BY $\langle 1 \rangle 2$ DEF *ThoseOver*, *ThoseUnder*
$\langle 2 \rangle 2$. $w = Supremum(S, Geq)$
BY DEF *Floor*, *ThoseUnder*
$\langle 2 \rangle 3$. $r = Infimum(S, Leq)$
BY $\langle 2 \rangle 1$ DEF *Ceil*, *ThoseOver*
$\langle 2 \rangle$ QED
BY $\langle 2 \rangle 2$, $\langle 2 \rangle 3$ DEF *Supremum*, *Infimum*
$\langle 1 \rangle$ QED
BY $\langle 1 \rangle 4$, $\langle 1 \rangle 5$

Similar to MaxFloorSmaller.
THEOREM $MaxCeilSmaller \triangleq$
ASSUME
NEW X, NEW Y, NEW Leq,
$IsFiniteSet(X)$
PROVE
LET
$R \triangleq MaxCeilings(X, Y, Leq)$
$T \triangleq Ceilings(X, Y, Leq)$
IN
$\land R \subseteq T$
$\land IsFiniteSet(R) \land IsFiniteSet(T)$
$\land Cardinality(R) \leq Cardinality(T)$
$\land Cardinality(T) \leq Cardinality(X)$
PROOF
$\langle 1 \rangle$ DEFINE

$R \triangleq MaxCeilings(X,\ Y,\ Leq)$
$T \triangleq Ceilings(X,\ Y,\ Leq)$
$\langle 1\rangle 1.\ R = Maxima(T,\ Leq)$
BY DEF $MaxCeilings$
$\langle 1\rangle 2.\ R \subseteq T$
BY $\langle 1\rangle 1$, $MaxIsSubset$
$\langle 1\rangle 3.\ \wedge\ IsFiniteSet(T)$
$\wedge\ Cardinality(T) \leq Cardinality(X)$
BY $ImageOfFinite$ DEF $Ceilings$
$\langle 1\rangle 4.\ \wedge\ IsFiniteSet(R)$
$\wedge\ Cardinality(R) \leq Cardinality(T)$
BY $\langle 1\rangle 2$, $\langle 1\rangle 3$, FS_Subset
$\langle 1\rangle$ QED
BY $\langle 1\rangle 2$, $\langle 1\rangle 3$, $\langle 1\rangle 4$, $FS\_CardinalityType$

Reasoning about the variant(termination).

THEOREM $FloorEqual \triangleq$
ASSUME
NEW Leq, NEW X, NEW Y, NEW $X0$, NEW $Y0$, NEW $y \in Y$,
$IsACompleteLattice(Leq)$,
LET $Z \triangleq Support(Leq)$
IN $\wedge\ X0 \subseteq Z$
$\wedge\ Y0 \subseteq Z$
$\wedge\ X \subseteq Z$
$\wedge\ Y \subseteq Z$
$\wedge\ IsFiniteSet(X0) \wedge IsFiniteSet(Y0)$
the next line should be provable from the above line
$\wedge\ IsFiniteSet(X) \wedge IsFiniteSet(Y)$
$\wedge\ X = MaxCeilings(X0,\ Y,\ Leq)$
$\wedge\ Y = MaxFloors(Y0,\ X0,\ Leq)$
$\wedge\ Cardinality(X) = Cardinality(X0)$
PROVE
$y = Floor(y,\ X,\ Leq)$
PROOF
$\langle 1\rangle$ DEFINE
$Z \triangleq Support(Leq)$
$RTX0 \triangleq Ceilings(X0,\ Y,\ Leq)$
$y0 \triangleq$ CHOOSE $r \in Y0 :\ y = Floor(r,\ X0,\ Leq)$
$S0 \triangleq ThoseUnder(X0,\ y0,\ Leq)$
$S1 \triangleq ThoseUnder(X0,\ y,\ Leq)$
$S2 \triangleq ThoseUnder(RTX0,\ y,\ Leq)$
$S \triangleq ThoseUnder(X,\ y,\ Leq)$
$a \triangleq Floor(y0,\ X0,\ Leq)$

$b \triangleq Floor(y,\ X,\ Leq)$
$c \triangleq Floor(y,\ X0,\ Leq)$
⟨1⟩1. $\wedge\ Floor(y0,\ X0,\ Leq) = Supremum(S0,\ Leq)$
$\wedge\ Floor(y,\ X0,\ Leq) = Supremum(S1,\ Leq)$
$\wedge\ Floor(y,\ X,\ Leq) = Supremum(S,\ Leq)$
BY DEF *Floor*
⟨1⟩2. $\wedge\ S0 \subseteq Z$
$\wedge\ S1 \subseteq Z$
$\wedge\ S \subseteq Z$
BY DEF *ThoseUnder*
⟨1⟩3. $\wedge\ a \in Z$
$\wedge\ b \in Z$
$\wedge\ c \in Z$
BY ⟨1⟩1, ⟨1⟩2, *SupExists*
⟨1⟩4. SUFFICES $Leq[y,\ b]$
⟨2⟩1. $Leq[b,\ y]$
BY *FloorIsSmaller*
⟨2⟩2. $IsAntiSymmetric(Leq)$
BY DEF *IsACompleteLattice*, *IsAPartialOrder*
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨1⟩3 DEF *IsAntiSymmetric*
⟨1⟩5. $y = Floor(y0,\ X0,\ Leq)$
⟨2⟩1. SUFFICES $\exists\, r \in Y0 :\ y = Floor(r,\ X0,\ Leq)$
OBVIOUS
⟨2⟩2. $Y = Maxima(Floors(Y0,\ X0,\ Leq),\ Leq)$
BY DEF *MaxFloors*
⟨2⟩3. $Y \subseteq Floors(Y0,\ X0,\ Leq)$
BY ⟨2⟩2, *MaxIsSubset*
⟨2⟩ QED
BY ⟨2⟩3 DEF *Floors*
⟨1⟩6. SUFFICES $Leq[a,\ b]$
BY ⟨1⟩5
⟨1⟩7. $X = Ceilings(X0,\ Y,\ Leq)$
⟨2⟩1. $X = Maxima(RTX0,\ Leq)$
BY DEF *MaxCeilings*
⟨2⟩2. $X \subseteq RTX0$
BY ⟨2⟩1, *MaxIsSubset*
⟨2⟩3. $Cardinality(RTX0) \leq Cardinality(X0)$
BY *ImageOfFinite* DEF *Ceilings*
⟨2⟩4. $Cardinality(X) \leq Cardinality(RTX0)$
BY ⟨2⟩2, *FS_Subset*, *MaxCeilSmaller*
⟨2⟩5. $Cardinality(X) = Cardinality(X0)$
OBVIOUS
⟨2⟩6. $Cardinality(X0) \leq Cardinality(RTX0)$
BY ⟨2⟩4, ⟨2⟩5

⟨2⟩7. $\land$ $IsFiniteSet(RTX0)$
$\land$ $Cardinality(X0) = Cardinality(RTX0)$
BY ⟨2⟩2, ⟨2⟩6, $MaxCeilSmaller$, $FS\_CardinalityType$
⟨2⟩8. $Cardinality(X) = Cardinality(RTX0)$
BY ⟨2⟩7
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩7, ⟨2⟩8, $MaxSame$
⟨1⟩8. $S0 \subseteq S1$
⟨2⟩1. SUFFICES $\forall\, x \in S0 :\ Leq[x,\ y]$
BY DEF $ThoseUnder$
⟨2⟩2. $y = Supremum(S0,\ Leq)$
BY ⟨1⟩1, ⟨1⟩5
⟨2⟩3. $IsAbove(y,\ S0,\ Leq)$
BY ⟨2⟩2, ⟨1⟩2, $SupExists$
⟨2⟩ QED
BY ⟨2⟩3 DEF $IsAbove$
⟨1⟩9. $Leq[a,\ c]$
BY ⟨1⟩8, ⟨1⟩1, ⟨1⟩2, $SupIsMonotonic$
⟨1⟩10. SUFFICES $Leq[c,\ b]$
⟨2⟩1. $Leq[a,\ c]$
BY ⟨1⟩9
⟨2⟩2. $Leq[c,\ b]$
BY ⟨1⟩10
⟨2⟩3. $IsTransitive(Leq)$
BY DEF $IsACompleteLattice$, $IsAPartialOrder$
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨1⟩3 DEF $IsTransitive$
⟨1⟩11. SUFFICES $Refines(S1,\ S,\ Leq)$
BY ⟨1⟩1, ⟨1⟩2, $SupOfRefinement$ DEF $Refines$
⟨1⟩12. SUFFICES $Refines(S1,\ S2,\ Leq)$
BY ⟨1⟩7
⟨1⟩13. SUFFICES $\forall\, u \in S1 :\ \exists\, v \in S2 :\ Leq[u,\ v]$
BY DEF $Refines$
⟨1⟩14. $\forall\, x \in S1 :\ Leq[x,\ y]$
BY DEF $ThoseUnder$
⟨1⟩15. $\forall\, x \in S1 :\ Leq[x,\ Ceil(x,\ Y,\ Leq)]$
BY ⟨1⟩2, $CeilIsLarger$
⟨1⟩16. $\forall\, x \in X0 :\ Ceil(x,\ Y,\ Leq) \in RTX0$
BY DEF $Ceilings$
⟨1⟩17. $\forall\, x \in X0 :$ LET $C \triangleq Ceil(x,\ Y,\ Leq)$
IN $Leq[x,\ y] \Rightarrow Leq[C,\ y]$
BY $CeilIsBelowThoseOver$
⟨1⟩18. $S1 \subseteq X0$
BY DEF $ThoseUnder$
⟨1⟩19. $\forall\, x \in S1 :$ LET $C \triangleq Ceil(x,\ Y,\ Leq)$

IN $Leq[C,\ y]$

BY $\langle 1\rangle 18$, $\langle 1\rangle 14$, $\langle 1\rangle 17$

$\langle 1\rangle 20.\ \forall\, x \in S1 :\ Ceil(x,\ Y,\ Leq) \in RTX0$

BY $\langle 1\rangle 18$, $\langle 1\rangle 19$ DEF $Ceilings$

$\langle 1\rangle 21.\ \forall\, x \in S1 :\ Ceil(x,\ Y,\ Leq) \in S2$

BY $\langle 1\rangle 19$, $\langle 1\rangle 20$ DEF $ThoseUnder$

$\langle 1\rangle$ QED

BY $\langle 1\rangle 15$, $\langle 1\rangle 21$

THEOREM $CeilEqual \triangleq$

ASSUME

NEW Leq, NEW X, NEW Y, NEW $X0$, NEW $Y0$, NEW $x \in X$,
$IsACompleteLattice(Leq)$,
LET $Z \triangleq Support(Leq)$
IN $\land X0 \subseteq Z$
$\land Y0 \subseteq Z$
$\land X \subseteq Z$
$\land Y \subseteq Z$
$\land IsFiniteSet(X0) \land IsFiniteSet(Y0)$
$\land IsFiniteSet(X) \land IsFiniteSet(Y)$
$\land X = MaxCeilings(X0,\ Y,\ Leq)$
$\land Y = MaxFloors(Y0,\ X0,\ Leq)$
$\land Cardinality(Y) = Cardinality(Y0)$

PROVE

$x = Ceil(x,\ Y,\ Leq)$

PROOF OMITTED *similar to proof of FloorEqual*

THEOREM $Fixpoint \triangleq$

ASSUME

NEW Leq, NEW X, NEW Y, NEW $X0$, NEW $Y0$,
$IsACompleteLattice(Leq)$,
LET $Z \triangleq Support(Leq)$
IN
$\land X0 \subseteq Z$
$\land Y0 \subseteq Z$
$\land X \subseteq Z$
$\land Y \subseteq Z$
$\land IsFiniteSet(X0) \land IsFiniteSet(Y0)$
The next line should be provable from the previous line.
$\land IsFiniteSet(X) \land IsFiniteSet(Y)$
$\land X = MaxCeilings(X0,\ Y,\ Leq)$
$\land Y = MaxFloors(Y0,\ X0,\ Leq)$
variant unchanged
$\land Cardinality(X) = Cardinality(X0)$

$\land\ Cardinality(Y) = Cardinality(Y0)$

PROVE

$\land\ X = MaxCeilings(X,\ Y,\ Leq)$

$\land\ Y = MaxFloors(Y,\ X,\ Leq)$

PROOF

$\langle 1\rangle 1.\ Y = MaxFloors(Y,\ X,\ Leq)$

$\langle 2\rangle 1.\ Y = Maxima(Y,\ Leq)$

BY *MaxIsIdempotent* DEF *MaxFloors*

$\langle 2\rangle 2.$ SUFFICES $Y = Floors(Y,\ X,\ Leq)$

BY $\langle 2\rangle 1$ DEF *MaxFloors*

$\langle 2\rangle 3.$ SUFFICES ASSUME NEW $y \in Y$

PROVE $y = Floor(y,\ X,\ Leq)$

BY $\langle 2\rangle 2$ DEF *Floors*

$\langle 2\rangle$ QED

BY *FloorEqual*

$\langle 1\rangle 2.\ X = MaxCeilings(X,\ Y,\ Leq)$

Proof similar to that of step $\langle 1\rangle 1$.

$\langle 2\rangle 1.\ X = Maxima(X,\ Leq)$

BY *MaxIsIdempotent* DEF *MaxCeilings*

$\langle 2\rangle 2.$ SUFFICES $X = Ceilings(X,\ Y,\ Leq)$

BY $\langle 2\rangle 1$ DEF *MaxCeilings*

$\langle 2\rangle 3.$ SUFFICES ASSUME NEW $x \in X$

PROVE $x = Ceil(x,\ Y,\ Leq)$

BY $\langle 2\rangle 2$ DEF *Ceilings*

$\langle 2\rangle$ QED

BY *CeilEqual*

$\langle 1\rangle$ QED

BY $\langle 1\rangle 1, \langle 1\rangle 2$

Removing essential elements is an isomorphism for the minimal covers.

$X \cap Y$ contains only essential elements.

PROPOSITION *CommonAreEssential* $\triangleq$

ASSUME

NEW *Leq*, NEW X, NEW Y, NEW C,

$IsACompleteLattice(Leq)$,

LET

$Z \triangleq Support(Leq)$

IN

$\land\ C \subseteq Y$

$\land\ X \subseteq Z$

$\land\ Y \subseteq Z$

$\land\ Y = Maxima(Y,\ Leq)$ *antichain*

$\land\ IsACover(C,\ X,\ Leq)$

PROVE
$(X \cap Y) \subseteq C$
PROOF
$\langle 1 \rangle 1$. SUFFICES $\forall\, u \in X \cap Y :\ \forall\, y \in Y :$
$Leq[u,\, y] \Rightarrow (u = y)$
BY DEF $IsACover$
$\langle 1 \rangle 2$. $IsAntiChain(Y,\, Leq)$
BY $LatticeProperties$, $MaximaIsAntiChain$
$\langle 1 \rangle$ QED
BY $\langle 1 \rangle 2$ DEF $IsAntiChain$

LEMMA $RemainsMinCoverAfterAddingEssential \triangleq$
ASSUME
NEW Leq, NEW X, NEW Y, NEW Ce,
$IsACompleteLattice(Leq)$,
LET
$Z \triangleq Support(Leq)$
$E \triangleq X \cap Y$
IN
$\land\, X \subseteq Z$
$\land\, Y \subseteq Z$
$\land\, X = Maxima(X,\, Leq)$
$\land\, Y = Maxima(Y,\, Leq)$
$\land\, IsAMinCover(Ce,\, X \setminus E,\, Y \setminus E,\, Leq)$
$\land\, IsFiniteSet(Z)$
$\land\, CardinalityAsCost(Z)$
PROVE
LET
$E \triangleq X \cap Y$
$C \triangleq Ce \cup E$
IN $IsAMinCover(C,\, X,\, Y,\, Leq)$
PROOF
$\langle 1 \rangle$ DEFINE
$Z \triangleq Support(Leq)$
$E \triangleq X \cap Y$
$Card(u) \triangleq Cardinality(u)$
$C \triangleq Ce \cup E$
$Xe \triangleq X \setminus E$
$Ye \triangleq Y \setminus E$
$\langle 1 \rangle 1$. SUFFICES ASSUME $\neg IsAMinCover(C,\, X,\, Y,\, Leq)$
PROVE FALSE
OBVIOUS
$\langle 1 \rangle 2$. $\land\, IsACover(Ce,\, Xe,\, Leq)$
$\land\, Ce \in$ SUBSET Ye

BY $MinCoverProperties$
$\langle 1 \rangle 3$. PICK $W \in$ SUBSET Y :
$\wedge \ IsACover(W, X, Leq)$
$\wedge \ CostLeq[\langle W, C \rangle]$
$\wedge \ \neg CostLeq[\langle C, W \rangle]$
$\langle 2 \rangle 1$. $IsACoverFrom(C, X, Y, Leq)$
$\langle 3 \rangle 1$. $IsACoverFrom(Ce, Xe, Ye, Leq)$
BY $\langle 1 \rangle 2$ DEF $IsACoverFrom$, $IsACover$
$\langle 3 \rangle 2$. $IsACoverFrom(C, Xe \cup E, Ye \cup E, Leq)$
BY $\langle 1 \rangle 2$, $\langle 3 \rangle 1$, $LatticeProperties$, $AddToBoth$
$\langle 3 \rangle$ QED
BY $\langle 3 \rangle 2$
$\langle 2 \rangle 2$. $C \in CoversOf(X, Y, Leq)$
BY $\langle 2 \rangle 1$ DEF $IsACoverFrom$, $CoversOf$
$\langle 2 \rangle$ HIDE DEF C
$\langle 2 \rangle$ QED
BY $\langle 1 \rangle 1$, $\langle 2 \rangle 2$, $CheaperCoverExists$
$\langle 1 \rangle$ DEFINE $We \triangleq W \setminus E$
$\langle 1 \rangle 4$. $We \in$ SUBSET Ye
BY $\langle 1 \rangle 3$
$\langle 1 \rangle 5$. $\wedge \ IsFiniteSet(W) \wedge IsFiniteSet(We)$
$\wedge \ IsFiniteSet(C) \ \wedge IsFiniteSet(Ce)$
$\wedge \ IsFiniteSet(E)$
$\langle 2 \rangle 1$. USE FS_Subset
$\langle 2 \rangle 2$. $IsFiniteSet(Ce)$
BY $\langle 1 \rangle 2$
$\langle 2 \rangle 3$. $IsFiniteSet(E)$
OBVIOUS
$\langle 2 \rangle 4$. $IsFiniteSet(C)$
BY $\langle 2 \rangle 2$, $\langle 2 \rangle 3$, FS_Union
$\langle 2 \rangle 5$. $IsFiniteSet(W)$
BY $\langle 1 \rangle 3$
$\langle 2 \rangle 6$. $IsFiniteSet(We)$
BY $\langle 2 \rangle 3$, $\langle 2 \rangle 5$
$\langle 2 \rangle$ QED
BY $\langle 2 \rangle 2$, $\langle 2 \rangle 3$, $\langle 2 \rangle 4$, $\langle 2 \rangle 5$, $\langle 2 \rangle 6$
$\langle 1 \rangle 6$. $\wedge \ Card(W) \ = Card(We) + Card(E)$
$\wedge \ Card(C) \ = Card(Ce) \ + Card(E)$
$\langle 2 \rangle 1$. $Card(W) = Card(We) + Card(E)$
$\langle 3 \rangle 1$. $W = We \cup E$
$\langle 4 \rangle 1$. $E \subseteq W$
BY $\langle 1 \rangle 3$, $CommonAreEssential$
$\langle 4 \rangle$ QED
BY $\langle 4 \rangle 1$
$\langle 3 \rangle 2$. $We \cap E = \{\}$

BY $\langle 1\rangle 4$

$\langle 3\rangle$ QED

BY $\langle 1\rangle 5$, $\langle 3\rangle 1$, $\langle 3\rangle 2$, *FS_UnionDisjoint*

$\langle 2\rangle 2$. $Card(C) = Card(Ce) + Card(E)$

$\langle 3\rangle 1$. $C = Ce \cup E$

OBVIOUS

$\langle 3\rangle 2$. $Ce \cap E = \{\}$

BY $\langle 1\rangle 2$

$\langle 3\rangle$ QED

BY $\langle 1\rangle 5$, $\langle 3\rangle 1$, $\langle 3\rangle 2$, *FS_UnionDisjoint*

$\langle 2\rangle$ QED

BY $\langle 2\rangle 1$, $\langle 2\rangle 2$

$\langle 1\rangle 7$. $\wedge\ C \in$ DOMAIN $Cost \wedge Ce \in$ DOMAIN $Cost$
$\wedge\ W \in$ DOMAIN $Cost \wedge We \in$ DOMAIN $Cost$

BY $\langle 1\rangle 2$, $\langle 1\rangle 3$ DEF *CardinalityAsCost*

$\langle 1\rangle 8$. $CostLeq[\langle We,\ Ce\rangle]$

$\langle 2\rangle 1$. USE DEF *CardinalityAsCost*, *CostLeq*

$\langle 2\rangle 2$. $CostLeq[\langle W,\ C\rangle]$

BY $\langle 1\rangle 3$

$\langle 2\rangle 3$. $Card(W) \leq Card(C)$

$\langle 3\rangle 1$. $\langle W,\ C\rangle \in$ DOMAIN *CostLeq*

BY $\langle 1\rangle 7$

$\langle 3\rangle 2$. $Cost[W] \leq Cost[C]$

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

$\langle 3\rangle$ QED

BY $\langle 1\rangle 7$, $\langle 3\rangle 2$

$\langle 2\rangle 4$. $Card(We) \leq Card(Ce)$

BY $\langle 1\rangle 5$, $\langle 1\rangle 6$, $\langle 2\rangle 3$, *FS_CardinalityType*

$\langle 2\rangle$ QED

$\langle 3\rangle 1$. $Cost[We] \leq Cost[Ce]$

BY $\langle 1\rangle 7$, $\langle 2\rangle 4$

$\langle 3\rangle 2$. $\langle We,\ Ce\rangle \in$ DOMAIN *CostLeq*

BY $\langle 1\rangle 7$

$\langle 3\rangle$ QED

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

$\langle 1\rangle 9$. $\neg CostLeq[\langle Ce,\ We\rangle]$

$\langle 2\rangle 1$. USE DEF *CardinalityAsCost*, *CostLeq*

$\langle 2\rangle 2$. SUFFICES ASSUME $CostLeq[\langle Ce,\ We\rangle]$
PROVE FALSE

OBVIOUS

$\langle 2\rangle 3$. $Card(Ce) \leq Card(We)$

$\langle 3\rangle 1$. $\langle Ce,\ We\rangle \in$ DOMAIN *CostLeq*

BY $\langle 1\rangle 7$, *CostLeqHelper*

$\langle 3\rangle 2$. $Cost[Ce] \leq Cost[We]$

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

⟨3⟩ QED
BY ⟨1⟩7, ⟨3⟩2
⟨2⟩4. $CostLeq[\langle C,\ W\rangle]$
⟨3⟩1. $\langle C,\ W\rangle \in$ DOMAIN $CostLeq$
BY ⟨1⟩7, $CostLeqHelper$
⟨3⟩2. $Card(C) \leq Card(W)$
BY ⟨2⟩3, ⟨1⟩6, ⟨1⟩5, $FS\_CardinalityType$
⟨3⟩3. $Cost[C] \leq Cost[W]$
BY ⟨1⟩7, ⟨3⟩2
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩3
⟨2⟩5. $\neg CostLeq[\langle C,\ W\rangle]$
BY ⟨1⟩3
⟨2⟩ QED
BY ⟨2⟩4, ⟨2⟩5
⟨1⟩10. $CostLeq[\langle Ce,\ We\rangle]$ *because C is a minimal cover and W is a cover that costs no more than C, so they must cost the same.*
⟨2⟩1. $\forall\, r \in$ SUBSET Ye :
$\lor \neg \land IsACover(r,\ Xe,\ Leq)$
$\land CostLeq[\langle r,\ Ce\rangle]$
$\lor CostLeq[\langle Ce,\ r\rangle]$
BY $MinCoverProperties$
⟨2⟩2. $We \in$ SUBSET Ye
BY ⟨1⟩4
⟨2⟩3. $IsACover(We,\ Xe,\ Leq)$
BY ⟨1⟩3, $SubtractFromBoth$, $LatticeProperties$
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨1⟩8
⟨1⟩ QED
BY ⟨1⟩9, ⟨1⟩10

LOCAL $PhantomProp(OtherCover,\ C,\ X,\ Leq) \triangleq$
$\land OtherCover \neq C$
$\land IsACover(OtherCover,\ X,\ Leq)$
$\land CostLeq[\langle OtherCover,\ C\rangle]$
$\land \neg CostLeq[\langle C,\ OtherCover\rangle]$

The following helps Isabelle check proof correctness.
THEOREM $CheaperCoverExistsHelper \triangleq$
ASSUME
NEW Leq, NEW X, NEW Y,
NEW $C \in CoversOf(X,\ Y,\ Leq)$, *so some cover exists*
$\neg IsAMinCover(C,\ X,\ Y,\ Leq)$

PROVE
$\exists\, OtherCover \in \text{SUBSET}\ Y :\ PhantomProp(OtherCover,\ C,\ X,\ Leq)$
PROOF
BY $CheaperCoverExists$ DEF $PhantomProp$

If C is a minimal cover of X,
then $C \setminus E$ is a minimal cover of $X \setminus E$
LEMMA $RemainsMinCoverAfterRemovingEssential \triangleq$
ASSUME
NEW Leq, NEW X, NEW Y, NEW C,
$IsACompleteLattice(Leq)$,
LET
$Z \triangleq Support(Leq)$
$E \triangleq X \cap Y$
IN
$\land\ X \subseteq Z$
$\land\ Y \subseteq Z$
$\land\ X = Maxima(X,\ Leq)$
$\land\ Y = Maxima(Y,\ Leq)$
$\land\ IsAMinCover(C,\ X,\ Y,\ Leq)$
$\land\ IsFiniteSet(Z)$
$\land\ CardinalityAsCost(Z)$
PROVE
LET
$E \triangleq X \cap Y$
$Xe \triangleq X \setminus E$
$Ye \triangleq Y \setminus E$
$Ce \triangleq C \setminus E$
IN
$IsAMinCover(Ce,\ Xe,\ Ye,\ Leq)$
PROOF
⟨1⟩ DEFINE
$Z \triangleq Support(Leq)$
$E \triangleq X \cap Y$
$Card(u) \triangleq Cardinality(u)$
$Ce \triangleq C \setminus E$
$Xe \triangleq X \setminus E$
$Ye \triangleq Y \setminus E$
⟨1⟩1. SUFFICES ASSUME $\neg IsAMinCover(Ce,\ Xe,\ Ye,\ Leq)$
PROVE FALSE
OBVIOUS
⟨1⟩2. $\land\ IsACover(C,\ X,\ Leq)$
$\land\ C \in \text{SUBSET}\ Y$
BY $MinCoverProperties$

⟨1⟩3. PICK $We \in \text{SUBSET } Ye$:
$\land\ IsACover(We, Xe, Leq)$
$\land\ CostLeq[\langle We, Ce\rangle]$
$\land\ \neg CostLeq[\langle Ce, We\rangle]$
⟨2⟩1. $IsACover(Ce, Xe, Leq)$
BY ⟨1⟩2, *SubtractFromBoth*, *LatticeProperties*
⟨2⟩2. $Ce \in \text{SUBSET } Ye$
BY *MinCoverProperties*
⟨2⟩3. $Ce \in CoversOf(Xe, Ye, Leq)$
BY ⟨2⟩1, ⟨2⟩2 DEF *CoversOf*
⟨2⟩ QED
Extra step to help Isabelle check the generated proofs.
⟨3⟩1. $\exists\, We \in \text{SUBSET } Ye :\ PhantomProp(We, Ce, Xe, Leq)$
BY ⟨1⟩1, ⟨2⟩3, *CheaperCoverExistsHelper*
⟨3⟩ QED
BY ⟨3⟩1 DEF *PhantomProp*
⟨1⟩ DEFINE $W \triangleq We \cup E$
⟨1⟩4. $IsACoverFrom(W, X, Y, Leq)$
⟨2⟩1. $IsACoverFrom(We, Xe, Ye, Leq)$
BY ⟨1⟩3 DEF *IsACoverFrom*
⟨2⟩2. $IsACoverFrom(We \cup E, Xe \cup E, Ye \cup E, Leq)$
BY ⟨2⟩1, *AddToBoth*, *LatticeProperties*
⟨2⟩3. $\land\ X = Xe \cup E$
$\land\ Y = Ye \cup E$
OBVIOUS
⟨2⟩ QED
BY ⟨2⟩2, ⟨2⟩3
⟨1⟩5. $\land\ IsFiniteSet(W) \land IsFiniteSet(We)$
$\land\ IsFiniteSet(C) \land IsFiniteSet(Ce)$
$\land\ IsFiniteSet(E)$
BY ⟨1⟩2, ⟨1⟩3, *FS_Subset*, *FS_Union*
⟨1⟩6. $\land\ Card(W) = Card(We) + Card(E)$
$\land\ Card(C) = Card(Ce) + Card(E)$
⟨2⟩1. USE *FS_UnionDisjoint*
⟨2⟩2. $Card(W) = Card(We) + Card(E)$
BY ⟨1⟩5
⟨2⟩3. $Card(C) = Card(Ce) + Card(E)$
⟨3⟩1. $E \subseteq C$
BY ⟨1⟩2, *CommonAreEssential*
⟨3⟩ QED
BY ⟨3⟩1, ⟨1⟩5
⟨2⟩ QED
BY ⟨2⟩2, ⟨2⟩3
⟨1⟩7. $\land\ C \in \text{DOMAIN } Cost \land Ce \in \text{DOMAIN } Cost$
$\land\ W \in \text{DOMAIN } Cost \land We \in \text{DOMAIN } Cost$

BY $\langle 1\rangle 2$, $\langle 1\rangle 3$ DEF *CardinalityAsCost*

$\langle 1\rangle 8$. *CostLeq*$[\langle W,\ C\rangle]$

$\langle 2\rangle$ USE DEF *CardinalityAsCost*, *CostLeq*

$\langle 2\rangle 1$. *CostLeq*$[\langle We,\ Ce\rangle]$

BY $\langle 1\rangle 3$

$\langle 2\rangle 2$. $Card(We) \leq Card(Ce)$

BY $\langle 1\rangle 7$, $\langle 2\rangle 1$

$\langle 2\rangle 3$. $Card(W) \leq Card(C)$

BY $\langle 2\rangle 2$, $\langle 1\rangle 6$, $\langle 1\rangle 5$, *FS_CardinalityType*

$\langle 2\rangle$ QED

$\langle 3\rangle 1$. $Cost[W] \leq Cost[C]$

BY $\langle 2\rangle 3$, $\langle 1\rangle 7$

$\langle 3\rangle 2$. $\langle W,\ C\rangle \in$ DOMAIN *CostLeq*

BY $\langle 1\rangle 7$

$\langle 3\rangle$ QED

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

$\langle 1\rangle 9$. $\neg$*CostLeq*$[\langle C,\ W\rangle]$

$\langle 2\rangle$ USE DEF *CardinalityAsCost*, *CostLeq*

$\langle 2\rangle 1$. SUFFICES ASSUME *CostLeq*$[\langle C,\ W\rangle]$
PROVE FALSE

OBVIOUS

$\langle 2\rangle 2$. $Card(C) \leq Card(W)$

BY $\langle 2\rangle 1$, $\langle 1\rangle 7$

$\langle 2\rangle 3$. *CostLeq*$[\langle Ce,\ We\rangle]$

$\langle 3\rangle 1$. $Card(Ce) \leq Card(We)$

BY $\langle 2\rangle 2$, $\langle 1\rangle 6$, $\langle 1\rangle 5$, *FS_CardinalityType*

$\langle 3\rangle$ QED

BY $\langle 3\rangle 1$, $\langle 1\rangle 7$

$\langle 2\rangle 4$. $\neg$*CostLeq*$[\langle Ce,\ We\rangle]$

BY $\langle 1\rangle 3$

$\langle 2\rangle$ QED

BY $\langle 2\rangle 3$, $\langle 2\rangle 4$

$\langle 1\rangle 10$. *CostLeq*$[\langle C,\ W\rangle]$

$\langle 2\rangle 1$. $\forall\, r \in$ SUBSET Y :
$\lor \neg \land$ *IsACover*$(r,\ X,\ Leq)$
$\land$ *CostLeq*$[\langle r,\ C\rangle]$
$\lor$ *CostLeq*$[\langle C,\ r\rangle]$

BY *MinCoverProperties*

$\langle 2\rangle 2$. $\land\ W \in$ SUBSET Y
$\land$ *IsACover*$(W,\ X,\ Leq)$

BY $\langle 1\rangle 4$ DEF *IsACoverFrom*

$\langle 2\rangle$ QED

BY $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 1\rangle 8$

$\langle 1\rangle$ QED

BY $\langle 1\rangle 9$, $\langle 1\rangle 10$

```
THEOREM MinCoverUnchangedByEssential ≜
  ASSUME
    NEW Leq, NEW X, NEW Y,
    NEW C, NEW Ce,
    IsACompleteLattice(Leq),
    LET
      Z ≜ Support(Leq)
      E ≜ X ∩ Y
    IN
      ∧ X ⊆ Z
      ∧ Y ⊆ Z
      ∧ X = Maxima(X, Leq)
      ∧ Y = Maxima(Y, Leq)
      ∧ IsFiniteSet(Z)
      ∧ CardinalityAsCost(Z)
      ∧ C = (Ce ∪ E)
      ∧ Ce = C \ E
  PROVE
    LET
      E ≜ X ∩ Y
      Xe ≜ X \ E
      Ye ≜ Y \ E
    IN
      IsAMinCover(C, X, Y, Leq) ≡ IsAMinCover(Ce, Xe, Ye, Leq)
  PROOF
  ⟨1⟩ DEFINE
      E ≜ X ∩ Y
      Xe ≜ X \ E
      Ye ≜ Y \ E
  ⟨1⟩1. ASSUME IsAMinCover(C, X, Y, Leq)
        PROVE IsAMinCover(Ce, Xe, Ye, Leq)
    ⟨2⟩1. Ce = C \ E
      OBVIOUS
    ⟨2⟩ QED
      BY ⟨1⟩1, ⟨2⟩1, RemainsMinCoverAfterRemovingEssential
  ⟨1⟩2. ASSUME IsAMinCover(Ce, Xe, Ye, Leq)
        PROVE IsAMinCover(C, X, Y, Leq)
    ⟨2⟩1. C = Ce ∪ E
      OBVIOUS
    ⟨2⟩ QED
      BY ⟨1⟩2, RemainsMinCoverAfterAddingEssential
  ⟨1⟩ QED
    BY ⟨1⟩1, ⟨1⟩2
```

Hat properties.

Above each element in a partially ordered finite set there exists some maximal element.

THEOREM $HasSomeMaximalAbove \triangleq$
ASSUME
NEW Leq, NEW S, NEW $u \in S$,
LET
$Z \triangleq Support(Leq)$
IN
$\land IsFiniteSet(Z)$
$\land S \subseteq Z$
$\land IsReflexive(Leq)$
$\land IsTransitive(Leq)$
$\land IsAntiSymmetric(Leq)$
PROVE
$\exists\, v \in S : \land Leq[u, v]$
$\land IsMaximal(v, S, Leq)$
PROOF
$\langle 1 \rangle$ DEFINE
$Z \triangleq Support(Leq)$
$Geq \triangleq UpsideDown(Leq)$
$W \triangleq Support(Geq)$
$\langle 1 \rangle 1. \land IsReflexive(Geq)$
$\land IsTransitive(Geq)$
$\land IsAntiSymmetric(Geq)$
$\land W = Z$
BY $SwapPreservesOrderProperties$, $UpsideDownHasSameSupport$
$\langle 1 \rangle 2.$ PICK $v \in S : \land Geq[v, u]$
$\land IsMinimal(v, S, Geq)$
BY $\langle 1 \rangle 1$, $HasSomeMinimalBelow$
$\langle 1 \rangle 3. Leq[u, v]$
BY $\langle 1 \rangle 2$, $LeqSwapOfGeq$
$\langle 1 \rangle 4. IsMaximal(v, S, Leq)$
$\langle 2 \rangle 1. \land v \in S$
$\land \forall\, q \in S : Geq[q, v] \Rightarrow Geq[v, q]$
BY $\langle 1 \rangle 2$ DEF $IsMinimal$
$\langle 2 \rangle 2. \forall\, q \in S : Leq[v, q] \Rightarrow Leq[q, v]$
BY $\langle 2 \rangle 1$, $LeqSwapOfGeq$
$\langle 2 \rangle$ QED
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$ DEF $IsMaximal$
$\langle 1 \rangle$ QED
BY $\langle 1 \rangle 3$, $\langle 1 \rangle 4$

Any subset Y of a partially ordered finite set Z can be mapped to its "MaxHat", made of maximal elements above each $y \in Y$

```
LEMMA HasMaxHat ≜
  ASSUME
    NEW Leq, NEW S, NEW Y,
    LET
      Z ≜ Support(Leq)
    IN
      ∧ IsAPartialOrder(Leq)
      ∧ IsFiniteSet(Z)
      ∧ S ⊆ Y
      ∧ Y ⊆ Z
  PROVE
    LET
      Max ≜ Maxima(Y, Leq)
    IN
      ∀ y ∈ S : ∃ ym ∈ Max : Leq[y, ym]
  PROOF
  ⟨1⟩1. ASSUME NEW y ∈ S
        PROVE ∃ ym ∈ Y : ∧ Leq[y, ym]
                         ∧ IsMaximal(ym, Y, Leq)
    ⟨2⟩1. y ∈ Y
      OBVIOUS
    ⟨2⟩ QED
      BY ⟨2⟩1, HasSomeMaximalAbove DEF IsAPartialOrder
  ⟨1⟩ QED
    BY ⟨1⟩1 DEF Maxima
```

H is smaller than S if any two of the selected maximal elements above different elements of P coincide.

```
PROPOSITION MaxHatProperties ≜
  ASSUME
    NEW Leq, NEW S, NEW Y,
    LET
      Z ≜ Support(Leq)
    IN
      ∧ IsAPartialOrder(Leq)
      ∧ IsFiniteSet(Z)
      ∧ S ⊆ Y
      ∧ Y ⊆ Z
  PROVE
    LET
      Max ≜ Maxima(Y, Leq)
      H ≜ MaxHat(S, Y, Leq)
```

IN

$\land$ $IsFiniteSet(H)$

$\land$ $H \in \text{SUBSET } Max$

$\land$ $Refines(S,\ H,\ Leq)$

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

PROOF

$\langle 1 \rangle$ DEFINE

$Max \triangleq Maxima(Y,\ Leq)$

$H \triangleq MaxHat(S,\ Y,\ Leq)$

$\langle 1 \rangle 1.\ IsFiniteSet(S)$

BY FS_Subset

$\langle 1 \rangle 2.\ \land\ IsFiniteSet(H)$

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

$\langle 2 \rangle$ DEFINE

$f \triangleq [u \in S \mapsto SomeMaxAbove(u,\ Y,\ Leq)]$

$\langle 2 \rangle 1.\ f \in Surjection(S,\ H)$

BY DEF $Surjection$, $MaxHat$

$\langle 2 \rangle$ QED

BY $\langle 2 \rangle 1$, $\langle 1 \rangle 1$, $FS\_Surjection$

$\langle 1 \rangle 3.\ \land\ H \in \text{SUBSET } Max$

$\land\ Refines(S,\ H,\ Leq)$

BY $HasMaxHat$ DEF $MaxHat$, $SomeMaxAbove$, $Refines$

$\langle 1 \rangle$ QED

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

THEOREM $MaxHatIsCoverToo \triangleq$

ASSUME

NEW Leq, NEW X, NEW S, NEW H,

LET

$Z \triangleq Support(Leq)$

IN

$\land\ IsTransitive(Leq)$

$\land\ IsFiniteSet(Z)$

$\land\ X \subseteq Z$

$\land\ S \subseteq Z$

$\land\ H \subseteq Z$

$\land\ Refines(S,\ H,\ Leq)$

$\land\ IsACover(S,\ X,\ Leq)$

PROVE

$IsACover(H,\ X,\ Leq)$

PROOF

$\langle 1 \rangle$ DEFINE

$Z \triangleq Support(Leq)$

$\langle 1 \rangle$ USE DEF $IsACover$

```
    ⟨1⟩1. SUFFICES ASSUME NEW u ∈ X
                   PROVE ∃ ym ∈ H : Leq[u, ym]
        OBVIOUS
    ⟨1⟩2. PICK y ∈ S : Leq[u, y]
        BY ⟨1⟩1
    ⟨1⟩3. PICK ym ∈ H : Leq[y, ym]
        BY DEF Refines
    ⟨1⟩4. ∧ u ∈ Z
          ∧ y ∈ Z
          ∧ ym ∈ Z
        BY ⟨1⟩1, ⟨1⟩2, ⟨1⟩3
    ⟨1⟩ QED
        BY ⟨1⟩2, ⟨1⟩3, ⟨1⟩4 DEF IsTransitive
```

Effect of MaxCeilings(X) on minimal covers.

Max(X) preserves covers.

```
LEMMA MaxPreservesCovers ≜
    ASSUME
        NEW Leq, NEW X, NEW Y, NEW C ∈ SUBSET Y,
        LET
            Z ≜ Support(Leq)
        IN
            ∧ IsFiniteSet(Z)
            ∧ IsAPartialOrder(Leq)
            ∧ X ⊆ Z
            ∧ Y ⊆ Z
    PROVE
        LET Max ≜ Maxima(X, Leq)
        IN  IsACover(C, X, Leq) ≡ IsACover(C, Max, Leq)
    PROOF
    ⟨1⟩ DEFINE
        Z ≜ Support(Leq)
        Max ≜ Maxima(X, Leq)
    ⟨1⟩1. ASSUME IsACover(C, X, Leq)
          PROVE IsACover(C, Max, Leq)
        BY ⟨1⟩1, MaxIsSubset DEF IsACover
    ⟨1⟩2. ASSUME IsACover(C, Max, Leq)
          PROVE IsACover(C, X, Leq)
        ⟨2⟩1. SUFFICES ASSUME NEW u ∈ X
                       PROVE ∃ y ∈ C : Leq[u, y]
            BY DEF IsACover
        ⟨2⟩2. PICK v ∈ X : Leq[u, v] ∧ IsMaximal(v, X, Leq)
            BY ⟨2⟩1, HasSomeMaximalAbove DEF IsAPartialOrder
```

```
        ⟨2⟩3. v ∈ Max
            BY ⟨2⟩2 DEF Maxima
        ⟨2⟩4. PICK y ∈ C : Leq[v, y]
            BY ⟨1⟩2, ⟨2⟩3 DEF IsACover
        ⟨2⟩5. Leq[u, y]
            ⟨3⟩1. (Z × Z) = DOMAIN Leq
                BY PartialOrderHasSymmetricDomain
            ⟨3⟩2. ∧ u ∈ Z
                  ∧ v ∈ Z
                  ∧ y ∈ Z
                BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩4
            ⟨3⟩3. Leq[u, v] ∧ Leq[v, y]
                BY ⟨2⟩2, ⟨2⟩4
            ⟨3⟩ QED
                BY ⟨3⟩2, ⟨3⟩3 DEF IsAPartialOrder, IsTransitive
        ⟨2⟩ QED
            BY ⟨2⟩5
    ⟨1⟩ QED
        BY ⟨1⟩1, ⟨1⟩2

Ceilings(X)preserves covers.
LEMMA CeilPreservesCovers ≜
    ASSUME
        NEW Leq, NEW X, NEW Y, NEW C ∈ SUBSET Y,
        LET
            Z ≜ Support(Leq)
        IN
            ∧ X ⊆ Z
            ∧ Y ⊆ Z
            ∧ IsACompleteLattice(Leq)
    PROVE
        LET Top ≜ Ceilings(X, Y, Leq)
        IN  IsACover(C, X, Leq) ≡ IsACover(C, Top, Leq)
    PROOF
    ⟨1⟩ DEFINE
        Z ≜ Support(Leq)
        Top ≜ Ceilings(X, Y, Leq)
    ⟨1⟩1. ASSUME IsACover(C, X, Leq)
          PROVE IsACover(C, Top, Leq)
        ⟨2⟩1. SUFFICES ASSUME NEW u ∈ Top
                       PROVE ∃ y ∈ C : Leq[u, y]
            BY DEF IsACover
        ⟨2⟩2. PICK r ∈ X : u = Ceil(r, Y, Leq)
            BY ⟨2⟩1 DEF Ceilings
```

```
    ⟨2⟩3. PICK y ∈ C : Leq[r, y]
      BY ⟨1⟩1 DEF IsACover
    ⟨2⟩ QED
      BY ⟨2⟩2, ⟨2⟩3, CeilIsBelowThoseOver
  ⟨1⟩2. ASSUME IsACover(C, Top, Leq)
        PROVE IsACover(C, X, Leq)
    ⟨2⟩1. SUFFICES ASSUME NEW r ∈ X
                   PROVE ∃ y ∈ C : Leq[r, y]
      BY DEF IsACover
    ⟨2⟩ DEFINE u ≜ Ceil(r, Y, Leq)
    ⟨2⟩2. Leq[r, u]
      BY ⟨2⟩1, CeilIsLarger
    ⟨2⟩3. PICK y ∈ C : Leq[u, y]
      ⟨3⟩1. u ∈ Top
        BY DEF Ceilings
      ⟨3⟩ QED
        BY ⟨3⟩1, ⟨1⟩2 DEF IsACover
    ⟨2⟩4. IsTransitive(Leq)
      BY LatticeProperties
    ⟨2⟩ QED
      ⟨3⟩1. ∧ r ∈ Z
            ∧ u ∈ Z
            ∧ y ∈ Z
        ⟨4⟩1. u ∈ Z
          BY ⟨2⟩1, InfExists DEF Ceil, ThoseOver
        ⟨4⟩ QED
          BY ⟨2⟩1, ⟨2⟩3, ⟨4⟩1
      ⟨3⟩2. Leq[r, u] ∧ Leq[u, y]
        BY ⟨2⟩2, ⟨2⟩3
      ⟨3⟩ QED
        BY ⟨3⟩1, ⟨3⟩2, ⟨2⟩4 DEF IsTransitive
  ⟨1⟩ QED
    BY ⟨1⟩1, ⟨1⟩2

MaxCeilings(X)preserves covers.
THEOREM MaxCeilPreservesCovers ≜
  ASSUME
    NEW Leq, NEW X, NEW Y, NEW C ∈ SUBSET Y,
    LET
      Z ≜ Support(Leq)
    IN
      ∧ IsFiniteSet(Z)
      ∧ IsACompleteLattice(Leq)
      ∧ X ⊆ Z
```

```
            ∧ Y ⊆ Z
    PROVE
        LET R ≜ MaxCeilings(X, Y, Leq)
        IN  IsACover(C, X, Leq) ≡ IsACover(C, R, Leq)
    PROOF
    ⟨1⟩ DEFINE
        Top ≜ Ceilings(X, Y, Leq)
        Max ≜ Maxima(Top, Leq)
        R ≜ MaxCeilings(X, Y, Leq)
    ⟨1⟩1. R = Max
        BY DEF MaxCeilings
    ⟨1⟩2. IsACover(C, X, Leq) ≡ IsACover(C, Top, Leq)
        BY CeilPreservesCovers
    ⟨1⟩3. IsACover(C, Top, Leq) ≡ IsACover(C, Max, Leq)
        ⟨2⟩1. Top ⊆ Support(Leq)
            BY InfExists DEF Ceilings, Ceil, ThoseOver
        ⟨2⟩2. IsAPartialOrder(Leq)
            BY DEF IsACompleteLattice
        ⟨2⟩ QED
            BY ⟨2⟩1, ⟨2⟩2, MaxPreservesCovers
    ⟨1⟩ QED
        BY ⟨1⟩1, ⟨1⟩2, ⟨1⟩3

THEOREM MinCoverUnchangedByMaxCeil ≜
    ASSUME
        NEW Leq, NEW X, NEW Y, NEW C ∈ SUBSET Y,
        LET
            Z ≜ Support(Leq)
        IN
            ∧ IsFiniteSet(Z)
            ∧ IsACompleteLattice(Leq)
            ∧ X ⊆ Z
            ∧ Y ⊆ Z
    PROVE
        LET R ≜ MaxCeilings(X, Y, Leq)
        IN  IsAMinCover(C, X, Y, Leq) ≡ IsAMinCover(C, R, Y, Leq)
    PROOF
    BY MaxCeilPreservesCovers DEF IsAMinCover, CoversOf
```

Effect of Maxima(Y) on minimal covers.

Soundness of Max(Y):
Every cover using elements from Max(Y) that is minimal within Max(Y) is a cover from Y minimal within Y.

```
LEMMA MinCoversFromMaxSuffice ≜
  ASSUME
    NEW Leq, NEW X, NEW Y, NEW C,
    LET
      Z ≜ Support(Leq)
      Max ≜ Maxima(Y, Leq)
    IN
      ∧ IsAPartialOrder(Leq)
      ∧ IsFiniteSet(Z)
      ∧ X ⊆ Z
      ∧ Y ⊆ Z
      ∧ IsAMinCover(C, X, Max, Leq)
      ∧ CardinalityAsCost(Z)
  PROVE
    IsAMinCover(C, X, Y, Leq)
  PROOF
  ⟨1⟩ DEFINE
      Z ≜ Support(Leq)
      Max ≜ Maxima(Y, Leq)
  ⟨1⟩1. ∧ C ∈ SUBSET Max
        ∧ IsACover(C, X, Leq)
        ∧ ∀ r ∈ SUBSET Max :
          ∨ ¬ ∧ IsACover(r, X, Leq)
              ∧ CostLeq[⟨r, C⟩]
          ∨ CostLeq[⟨C, r⟩]
      BY MinCoverProperties
  ⟨1⟩2. ∧ C ∈ SUBSET Max
        ∧ Max ∈ SUBSET Y
      BY ⟨1⟩1, MaxIsSubset
  ⟨1⟩3. SUFFICES ASSUME ¬IsAMinCover(C, X, Y, Leq)
                 PROVE FALSE
      OBVIOUS
  ⟨1⟩4. PICK P ∈ SUBSET Y :
          ∧ IsACover(P, X, Leq)
          ∧ CostLeq[⟨P, C⟩]
          ∧ ¬CostLeq[⟨C, P⟩]
        ⟨2⟩1. C ∈ CoversOf(X, Y, Leq)
          ⟨3⟩1. C ∈ SUBSET Y
            BY ⟨1⟩2
          ⟨3⟩2. IsACover(C, X, Leq)
            BY ⟨1⟩1
          ⟨3⟩ QED
            BY ⟨3⟩1, ⟨3⟩2 DEF CoversOf
        ⟨2⟩ QED
          BY ⟨2⟩1, ⟨1⟩3, CheaperCoverExists
```

⟨1⟩ DEFINE $Pm \triangleq MaxHat(P,\ Y,\ Leq)$
⟨1⟩5. $\land\ Pm \in$ SUBSET Max
$\land\ \forall\, y \in P :\ \exists\, ym \in Pm :\ Leq[y,\ ym]$
$\land\ Cardinality(Pm) \leq Cardinality(P)$
BY $MaxHatProperties$ DEF $Refines$
⟨1⟩6. $\land\ IsFiniteSet(C) \land (Cardinality(C) \in Nat)$
$\land\ IsFiniteSet(P) \land (Cardinality(P) \in Nat)$
$\land\ IsFiniteSet(Pm) \land (Cardinality(Pm) \in Nat)$
⟨2⟩1. $C \in$ SUBSET Z
BY ⟨1⟩2
⟨2⟩2. $P \in$ SUBSET Z
BY ⟨1⟩4
⟨2⟩3. $Pm \in$ SUBSET Z
BY ⟨1⟩5, ⟨1⟩2
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, FS_Subset, $FS\_CardinalityType$
⟨1⟩7. $\land\ C \in$ DOMAIN $Cost$
$\land\ P \in$ DOMAIN $Cost$
$\land\ Pm \in$ DOMAIN $Cost$
BY ⟨1⟩2, ⟨1⟩4, ⟨1⟩5 DEF $CardinalityAsCost$
⟨1⟩8. $IsACover(Pm,\ X,\ Leq)$
⟨2⟩1. $IsTransitive(Leq)$
BY DEF $IsAPartialOrder$
⟨2⟩2. $IsACover(P,\ X,\ Leq)$
BY ⟨1⟩4
⟨2⟩3. $P \subseteq Z \land Pm \subseteq Z$
⟨3⟩1. SUBSET $Z =$ DOMAIN $Cost$
BY DEF $CardinalityAsCost$
⟨3⟩ QED
BY ⟨1⟩7, ⟨3⟩1
⟨2⟩4. $Refines(P,\ Pm,\ Leq)$
BY ⟨1⟩5 DEF $Refines$
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, $MaxHatIsCoverToo$
⟨1⟩9. $CostLeq[\langle Pm,\ C\rangle]$
⟨2⟩1. $CostLeq[\langle P,\ C\rangle]$
BY ⟨1⟩4
⟨2⟩ USE DEF $CardinalityAsCost$, $CostLeq$
⟨2⟩2. $Cardinality(P) \leq Cardinality(C)$
BY ⟨2⟩1, ⟨1⟩7
⟨2⟩3. $Cardinality(Pm) \leq Cardinality(C)$
BY ⟨2⟩2, ⟨1⟩5, ⟨1⟩6
⟨2⟩ QED
BY ⟨2⟩3, ⟨1⟩7
⟨1⟩10. $\neg CostLeq[\langle C,\ Pm\rangle]$

⟨2⟩1. $\neg CostLeq[\langle C,\ P\rangle]$
BY ⟨1⟩4
⟨2⟩ USE DEF $CardinalityAsCost,\ CostLeq$
⟨2⟩2. $\neg(Cardinality(C) \leq Cardinality(P))$
BY ⟨2⟩1, ⟨1⟩7
⟨2⟩3. $Cardinality(C) > Cardinality(P)$
BY ⟨2⟩2, ⟨1⟩6
⟨2⟩4. $Cardinality(C) > Cardinality(Pm)$
BY ⟨2⟩3, ⟨1⟩5, ⟨1⟩6
⟨2⟩5. $\neg(Cardinality(C) \leq Cardinality(Pm))$
BY ⟨2⟩4, ⟨1⟩6
⟨2⟩ QED
BY ⟨2⟩5, ⟨1⟩7
⟨1⟩ QED
⟨2⟩1. $CostLeq[\langle C,\ Pm\rangle]$
⟨3⟩1. $Pm \in$ SUBSET Max
BY ⟨1⟩5
⟨3⟩2. $IsACover(Pm,\ X,\ Leq)$
BY ⟨1⟩8
⟨3⟩3. $CostLeq[\langle Pm,\ C\rangle]$
BY ⟨1⟩9
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨1⟩1
⟨2⟩ QED
BY ⟨2⟩1, ⟨1⟩10

Completeness of $Max(Y)$:
For each cover from Y minimal within Y, there exists a cover from $Max(Y)$ minimal in $Max(Y)$.So, if a minimal cover from Y exists, then a minimal cover from $Max(Y)$also exists.

LEMMA $MaxHatOfMinCoverIsAMinCover \triangleq$
ASSUME
NEW Leq, NEW X, NEW Y, NEW C,
LET
$Z \triangleq Support(Leq)$
IN
$\wedge\ IsAPartialOrder(Leq)$
$\wedge\ IsFiniteSet(Z)$
$\wedge\ X \subseteq Z$
$\wedge\ Y \subseteq Z$
$\wedge\ IsAMinCover(C,\ X,\ Y,\ Leq)$
$\wedge\ CardinalityAsCost(Z)$
PROVE
LET

$Max \triangleq Maxima(Y, Leq)$
$Cm \triangleq MaxHat(C, Y, Leq)$
IN
$IsAMinCover(Cm, X, Max, Leq)$
PROOF
⟨1⟩ DEFINE
$Z \triangleq Support(Leq)$
$Max \triangleq Maxima(Y, Leq)$
⟨1⟩1. $\land C \in$ SUBSET Y
$\land IsACover(C, X, Leq)$
$\land \forall r \in$ SUBSET Y :
$\lor \neg \land IsACover(r, X, Leq)$
$\land CostLeq[\langle r, C\rangle]$
$\lor CostLeq[\langle C, r\rangle]$
BY $MinCoverProperties$
⟨1⟩2. $IsFiniteSet(C)$
BY ⟨1⟩1, FS_Subset
⟨1⟩3. DEFINE $Cm \triangleq MaxHat(C, Y, Leq)$
⟨1⟩4. $\land IsFiniteSet(Cm)$
$\land Cm \in$ SUBSET Max
$\land Refines(C, Cm, Leq)$
$\land Cardinality(Cm) \leq Cardinality(C)$
BY ⟨1⟩1, $MaxHatProperties$
⟨1⟩5. $\land C \in$ SUBSET Z
$\land Cm \in$ SUBSET Z
BY ⟨1⟩1, ⟨1⟩4, $MaxIsSubset$
⟨1⟩6. $IsACover(Cm, X, Leq)$
BY ⟨1⟩4, ⟨1⟩1, ⟨1⟩5, $MaxHatIsCoverToo$ DEF $IsAPartialOrder$
⟨1⟩7. $Cardinality(Cm) = Cardinality(C)$
⟨2⟩ USE DEF $CardinalityAsCost$, $CostLeq$
⟨2⟩1. $CostLeq[\langle Cm, C\rangle]$
⟨3⟩1. $Max \in$ SUBSET Y
BY $MaxIsSubset$
⟨3⟩2. $\land Cm \in$ DOMAIN $Cost$
$\land C \in$ DOMAIN $Cost$
BY ⟨1⟩1, ⟨1⟩4, ⟨3⟩1
⟨3⟩ QED
BY ⟨1⟩4, ⟨3⟩2 DEF $CostLeq$
⟨2⟩2. $CostLeq[\langle C, Cm\rangle]$
⟨3⟩1. $Cm \in$ SUBSET Y
BY ⟨1⟩4, $MaxIsSubset$
⟨3⟩2. $\land IsACover(Cm, X, Leq)$
$\land CostLeq[\langle Cm, C\rangle]$
BY ⟨1⟩6, ⟨2⟩1
⟨3⟩ QED

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

$\langle 2\rangle 3$. $\wedge\ Cardinality(Cm) \leq Cardinality(C)$
$\wedge\ Cardinality(Cm) \geq Cardinality(C)$
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 1\rangle 5$

$\langle 2\rangle 4$. $\wedge\ Cardinality(Cm) \in Nat$
$\wedge\ Cardinality(C) \in Nat$
BY $\langle 1\rangle 2$, $\langle 1\rangle 4$, $FS\_CardinalityType$

$\langle 2\rangle$ QED
BY $\langle 2\rangle 3$, $\langle 2\rangle 4$

$\langle 1\rangle 8$. ASSUME NEW $r \in$ SUBSET Max,
$\wedge\ IsACover(r, X, Leq)$
$\wedge\ CostLeq[\langle r, Cm\rangle]$
PROVE $CostLeq[\langle Cm, r\rangle]$

$\langle 2\rangle$ USE DEF $CardinalityAsCost$, $CostLeq$

$\langle 2\rangle 1$. $r \in$ SUBSET Y
BY $\langle 1\rangle 8$, $MaxIsSubset$

$\langle 2\rangle 2$. $CostLeq[\langle r, C\rangle]$

$\langle 3\rangle 1$. $Cardinality(r) \leq Cardinality(Cm)$
BY $\langle 1\rangle 8$, $\langle 1\rangle 5$, $\langle 2\rangle 1$

$\langle 3\rangle 2$. $Cardinality(r) \leq Cardinality(C)$
BY $\langle 3\rangle 1$, $\langle 1\rangle 7$

$\langle 3\rangle$ QED
BY $\langle 3\rangle 2$, $\langle 1\rangle 5$, $\langle 2\rangle 1$

$\langle 2\rangle 3$. $CostLeq[\langle C, r\rangle]$
BY $\langle 1\rangle 1$, $\langle 1\rangle 8$, $\langle 2\rangle 1$, $\langle 2\rangle 2$

$\langle 2\rangle$ QED

$\langle 3\rangle 1$. $Cardinality(C) \leq Cardinality(r)$
BY $\langle 2\rangle 3$, $\langle 1\rangle 5$, $\langle 2\rangle 1$

$\langle 3\rangle 2$. $Cardinality(Cm) \leq Cardinality(r)$
BY $\langle 3\rangle 1$, $\langle 1\rangle 7$

$\langle 3\rangle$ QED
BY $\langle 3\rangle 2$, $\langle 1\rangle 5$, $\langle 2\rangle 1$

$\langle 1\rangle$ QED
BY $\langle 1\rangle 4$, $\langle 1\rangle 6$, $\langle 1\rangle 8$ DEF $IsAMinCover$, $IsMinimal$, $CoversOf$

Floor effects on minimal covers.

PROPOSITION $UnfloorProperties \triangleq$
ASSUME
NEW Leq, NEW X, NEW Y, NEW u,
$\wedge\ IsACompleteLattice(Leq)$
$\wedge\ u \in Floors(Y, X, Leq)$
PROVE
LET $y \triangleq SomeUnfloor(u, X, Y, Leq)$

IN
$\land\ y \in Y$
$\land\ u = Floor(y,\ X,\ Leq)$
PROOF
$\langle 1\rangle 1.\ \exists\, y \in Y :\ u = Floor(y,\ X,\ Leq)$
BY DEF *Floors*
$\langle 1\rangle$ QED
BY $\langle 1\rangle 1$ DEF *SomeUnfloor*

$Cf = Floors(Unfloors(Cf))$.
But it is possible that $C \neq Unfloors(Floors(C))$.

The cause is that different elements in C can have the same Floor.
So for two elements $y1,\ y2 \in C$ it can be $r \triangleq Floor(y1) = Floor(y2)$,
but $Unfloor(r)$will be a choice of one of $y1$ or $y2$.
The choice is arbitrary, because Unfloor is defined using CHOOSE .

PROPOSITION *UnfloorSetProperties* $\triangleq$
ASSUME
NEW *Leq*, NEW *X*, NEW *Y*, NEW *Cf*,
$\land\ IsACompleteLattice(Leq)$
$\land\ Cf \subseteq Floors(Y,\ X,\ Leq)$
PROVE
LET $C \triangleq Unfloors(Cf,\ X,\ Y,\ Leq)$
IN
$\land\ Cf = Floors(C,\ X,\ Leq)$
$\land\ C \subseteq Y$
PROOF
$\langle 1\rangle$ DEFINE
$C \triangleq Unfloors(Cf,\ X,\ Y,\ Leq)$
$\langle 1\rangle 1.$ SUFFICES ASSUME NEW $u \in Cf$
PROVE $\exists\, y \in Y :\ u = Floor(y,\ X,\ Leq)$
BY $\langle 1\rangle 1$ DEF *Floors*, *Unfloors*, *SomeUnfloor*
$\langle 1\rangle$ QED
BY *UnfloorProperties*

The assumption $IsAntiChain(Cf,\ Leq) \land Cf \subseteq Floors(Y,\ X,\ Leq)$
does not suffice in the following proposition, because Cf can be an
antichain of elements that are not maximal within $Floors(Y,\ X,\ Leq)$.
In that case, $Leq[z,\ fy]$does not contradict the antichain property,
because fy is outside the set of comparison(in that case the antichain).

PROPOSITION *MaxFloorsHatIsUnfloor* $\triangleq$
ASSUME
NEW *Leq*, NEW *X*, NEW *Y*, NEW *Cf*,
LET
$Z \triangleq Support(Leq)$

IN

$\land X \subseteq Z \land Y \subseteq Z$

so that Floor exist

$\land IsACompleteLattice(Leq)$

$\land IsFiniteSet(Cf)$

ensures that each $z \in Cf$ is below some $y \in Y$
and that elements in Cf are maximal within Floors

$\land Cf \subseteq MaxFloors(Y, X, Leq)$

PROVE

LET

$C \triangleq Hat(Cf, Y, Leq)$

IN

$\land Cf = Floors(C, X, Leq)$

$\land Cardinality(Cf) = Cardinality(C)$

IsUnfloors is slightly weaker.

PROOF

$\langle 1 \rangle$ DEFINE

$Z \triangleq Support(Leq)$

$C \triangleq Hat(Cf, Y, Leq)$

$Yf \triangleq Floors(Y, X, Leq)$

$F \triangleq Floors(C, X, Leq)$

$Card(S) \triangleq Cardinality(S)$

$\langle 1 \rangle 1.$ $IsFiniteSet(C)$

BY *ImageOfFinite* DEF *Hat*

$\langle 1 \rangle 2.$ $\land Cf \subseteq Maxima(Yf, Leq)$
$\land Cf \subseteq Yf$
$\land Yf \subseteq Z$

$\langle 2 \rangle 1.$ $Cf \subseteq Maxima(Yf, Leq)$

BY DEF *MaxFloors*

$\langle 2 \rangle 2.$ $Cf \subseteq Yf$

BY $\langle 2 \rangle 1$, *MaxIsSubset*

$\langle 2 \rangle 3.$ $Yf \subseteq Z$

BY *FloorExists* DEF *Floors*

$\langle 2 \rangle$ QED

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

$\langle 1 \rangle 3.$ $\forall z \in Cf : \exists y \in Y : z = Floor(y, X, Leq)$

BY $\langle 1 \rangle 2$ DEF *Floors*

$\langle 1 \rangle 4.$ $\forall z \in Cf : \exists y \in Y : Leq[z, y]$

BY $\langle 1 \rangle 3$, *FloorIsSmaller*

$\langle 1 \rangle 5.$ $\forall z \in Cf : \exists y \in C : Leq[z, y]$

BY $\langle 1 \rangle 4$ DEF *Hat*, *SomeAbove*

$\langle 1 \rangle 6.$ $\forall y \in C : \exists z \in Cf : Leq[z, y]$

BY $\langle 1 \rangle 4$ DEF *Hat*, *SomeAbove*

$\langle 1 \rangle 7.$ $C \subseteq Y$

BY $\langle 1 \rangle 4$ DEF *Hat*, *SomeAbove*

⟨1⟩8. $F \subseteq Yf$
BY ⟨1⟩7 DEF $MaxFloors$, $Floors$
⟨1⟩9. $Cf = F$
⟨2⟩1. ASSUME NEW $z \in Cf$, NEW $y \in C$, NEW $fy \in F$,
$\land\ Leq[z,\ y]$
$\land\ fy = Floor(y,\ X,\ Leq)$
PROVE $z = fy$
Essentially the "conversely" *in Coudert* s Lemma 3.
⟨3⟩ DEFINE $fz \triangleq Floor(z,\ X,\ Leq)$
⟨3⟩1. $Leq[z,\ fy]$
⟨4⟩1. $(z \in Z) \land (y \in Z)$
BY ⟨2⟩1, ⟨1⟩2, ⟨2⟩1, ⟨1⟩7
⟨4⟩2. $Leq[fz,\ fy]$
BY ⟨2⟩1, ⟨4⟩1, *FloorIsMonotonic*
⟨4⟩3. $z = fz$
BY ⟨1⟩3, ⟨4⟩1, *FloorIsIdempotent*
⟨4⟩ QED
BY ⟨4⟩2, ⟨4⟩3
⟨3⟩2. $z \in Maxima(Yf,\ Leq)$
BY ⟨2⟩1, ⟨1⟩2
⟨3⟩3. $fy \in Yf$
BY ⟨2⟩1, ⟨1⟩8
⟨3⟩4. $Leq[fy,\ z]$
BY ⟨3⟩2, ⟨3⟩3, ⟨3⟩1, *MaximaProperties*
⟨3⟩5. $Leq[fy,\ z] \land Leq[z,\ fy]$
BY ⟨3⟩4, ⟨3⟩1
⟨3⟩6. $fy \in Z$
BY ⟨3⟩3, ⟨1⟩2
⟨3⟩7. $(fy \in Z) \land (z \in Z)$
BY ⟨3⟩6, ⟨2⟩1, ⟨1⟩2
⟨3⟩8. $IsAntiSymmetric(Leq)$
BY *LatticeProperties*
⟨3⟩ QED
BY ⟨3⟩5, ⟨3⟩8, ⟨3⟩7 DEF *IsAntiSymmetric*
⟨2⟩2. $Cf \subseteq F$
⟨3⟩1. SUFFICES ASSUME NEW $z \in Cf$
PROVE $z \in F$
OBVIOUS
⟨3⟩2. PICK $y \in C :\ Leq[z,\ y]$
BY ⟨3⟩1, ⟨1⟩5
⟨3⟩ DEFINE $fy \triangleq Floor(y,\ X,\ Leq)$
⟨3⟩3. $fy \in F$
BY DEF *Floors*
⟨3⟩4. SUFFICES $z = fy$
BY ⟨3⟩3

⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨2⟩1
⟨2⟩3. $F \subseteq Cf$
⟨3⟩1. SUFFICES ASSUME NEW $fy \in F$
PROVE $fy \in Cf$
OBVIOUS
⟨3⟩2. PICK $y \in C : fy = Floor(y, X, Leq)$
BY ⟨3⟩1 DEF *Floors*
⟨3⟩3. PICK $z \in Cf : Leq[z, y]$
BY ⟨3⟩2, ⟨1⟩6
⟨3⟩4. SUFFICES $z = fy$
BY ⟨3⟩3
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩3, ⟨3⟩2, ⟨2⟩1
⟨2⟩ QED
BY ⟨2⟩2, ⟨2⟩3
⟨1⟩10. $Card(Cf) = Card(C)$
⟨2⟩1. $Card(Cf) \leq Card(C)$
⟨3⟩ HIDE DEF C
⟨3⟩ QED
BY ⟨1⟩9, ⟨1⟩1, *ImageOfFinite* DEF *Floors*
⟨2⟩2. $Card(C) \leq Card(Cf)$
BY *ImageOfFinite* DEF *Hat*
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨1⟩1, *FS_CardinalityType*
⟨1⟩ QED
BY ⟨1⟩9, ⟨1⟩10

Effect of *Floor on covers.*

THEOREM *FloorPreservesCover* $\triangleq$
ASSUME
NEW *Leq*, NEW *X*, NEW *Y*, NEW *C*, NEW *Cf*,
LET
$Z \triangleq Support(Leq)$
IN
$\land X \subseteq Z \land Y \subseteq Z$
$\land C \subseteq Z$
$\land IsACompleteLattice(Leq)$
$\land Cf = Floors(C, X, Leq)$
PROVE
$IsACover(C, X, Leq) \equiv IsACover(Cf, X, Leq)$
PROOF
⟨1⟩ DEFINE

$Z \triangleq Support(Leq)$
⟨1⟩ $Cf \subseteq Z$
BY $FloorsIsSubset$
⟨1⟩1. ASSUME $IsACover(C, X, Leq)$
PROVE $IsACover(Cf, X, Leq)$
⟨2⟩1. SUFFICES ASSUME NEW $u \in X$
PROVE $\exists\, y \in Cf : Leq[u, y]$
BY DEF $IsACover$
⟨2⟩2. PICK $v \in C : Leq[u, v]$
BY ⟨1⟩1 DEF $IsACover$
⟨2⟩ DEFINE $y \triangleq Floor(v, X, Leq)$
⟨2⟩3. $Leq[u, y]$
BY ⟨2⟩1, ⟨2⟩2, $FloorIsAboveThoseUnder$
⟨2⟩4. $y \in Cf$
BY DEF $Floors$
⟨2⟩ QED
BY ⟨2⟩3, ⟨2⟩4
⟨1⟩2. ASSUME $IsACover(Cf, X, Leq)$
PROVE $IsACover(C, X, Leq)$
⟨2⟩1. SUFFICES ASSUME NEW $u \in X$
PROVE $\exists\, y \in C : Leq[u, y]$
BY DEF $IsACover$
⟨2⟩2. PICK $v \in Cf : Leq[u, v]$
BY ⟨1⟩2 DEF $IsACover$
⟨2⟩3. PICK $y \in C : v = Floor(y, X, Leq)$
BY DEF $Floors$
⟨2⟩4. $Leq[v, y]$
⟨3⟩1. $v \in Z \land y \in Z$
BY ⟨2⟩2, ⟨2⟩3
⟨3⟩2. $v = Floor(y, X, Leq)$
BY ⟨2⟩3
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, $FloorIsSmaller$
⟨2⟩ QED
⟨3⟩1. $Leq[u, v]$
BY ⟨2⟩2
⟨3⟩2. $Leq[v, y]$
BY ⟨2⟩4
⟨3⟩3. $IsTransitive(Leq)$
BY $LatticeProperties$
⟨3⟩4. $u \in Z \land v \in Z \land y \in Z$
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4 DEF $IsTransitive$
⟨1⟩ QED

BY $\langle 1\rangle 1$, $\langle 1\rangle 2$

A more general version of the next corollary can be proved about Hat, by a proof similar to MaxHatIsCoverToo

COROLLARY $UnfloorPreservesCover \triangleq$
ASSUME
NEW Leq, NEW X, NEW Y, NEW Cf, NEW C,
LET
$Z \triangleq Support(Leq)$
IN
$\land X \subseteq Z \land Y \subseteq Z$
$\land C \subseteq Z \land Cf \subseteq Z$
$\land IsACompleteLattice(Leq)$
$\land IsACover(Cf, X, Leq)$
$\land Cf = Floors(C, X, Leq)$
PROVE
$IsACover(C, X, Leq)$
PROOF
BY $FloorPreservesCover$

Effect of Floor on minimal covers.

LEMMA $FloorPreservesMinCover \triangleq$
ASSUME
NEW Leq, NEW X, NEW Y, NEW C,
LET
$Z \triangleq Support(Leq)$
IN
$\land IsACompleteLattice(Leq)$
$\land CardinalityAsCost(Z)$
$\land X \subseteq Z$
$\land Y \subseteq Z \land IsFiniteSet(Y)$ *Finiteness of Y*
may be avoidable, but of Yf appears to be necessary.
$\land C \subseteq Y$
$\land IsAMinCover(C, X, Y, Leq)$
PROVE
LET
$Cf \triangleq Floors(C, X, Leq)$
$Yf \triangleq Floors(Y, X, Leq)$
IN
$IsAMinCover(Cf, X, Yf, Leq)$
PROOF
$\langle 1\rangle$ DEFINE

$Z \triangleq Support(Leq)$
$Cf \triangleq Floors(C, X, Leq)$
$Yf \triangleq Floors(Y, X, Leq)$
$Card(S) \triangleq Cardinality(S)$
⟨1⟩ $IsFiniteSet(C)$
BY FS_Subset
⟨1⟩1. $\wedge\ Cf \subseteq Z$
$\wedge\ Yf \subseteq Z$
BY $FloorsIsSubset$
⟨1⟩2. $\wedge\ IsFiniteSet(Cf) \wedge IsFiniteSet(Yf)$
$\wedge\ Card(Cf) \leq Card(C)$
BY $FloorsSmaller$
⟨1⟩3. $\wedge\ IsACover(C, X, Leq)$
$\wedge\ C \in$ SUBSET Y
$\wedge\ \forall\, r \in$ SUBSET Y :
$\wedge\ IsACover(r, X, Leq)$
$\wedge\ CostLeq[\langle r, C\rangle]$
$\Rightarrow\ CostLeq[\langle C, r\rangle]$
BY $MinCoverProperties$
⟨1⟩4. SUFFICES ASSUME $\neg IsAMinCover(Cf, X, Yf, Leq)$
PROVE FALSE
OBVIOUS
⟨1⟩5. PICK $Wf \in$ SUBSET Yf :
$\wedge\ IsACover(Wf, X, Leq)$
$\wedge\ CostLeq[\langle Wf, Cf\rangle]$
$\wedge\ \neg CostLeq[\langle Cf, Wf\rangle]$
⟨2⟩1. $Cf \in CoversOf(X, Yf, Leq)$
⟨3⟩ $IsACover(Cf, X, Leq)$
BY ⟨1⟩3, $FloorPreservesCover$
⟨3⟩ $Cf \in$ SUBSET Yf
BY ⟨1⟩3, $FloorsIsSubset$ DEF $Floors$
⟨3⟩ QED
BY DEF $CoversOf$
⟨2⟩ QED
BY ⟨1⟩4, ⟨2⟩1, $CheaperCoverExists$
⟨1⟩6. $\wedge\ IsFiniteSet(Wf)$
$\wedge\ Card(Wf) \leq Card(Cf)$
⟨2⟩ $Card(Wf) \leq Card(Cf)$
BY ⟨1⟩5, ⟨1⟩1 DEF $CardinalityAsCost$, $CostLeq$
⟨2⟩ $IsFiniteSet(Wf)$
BY ⟨1⟩5, ⟨1⟩2, FS_Subset
⟨2⟩ QED
OBVIOUS
⟨1⟩ DEFINE $W \triangleq Unfloors(Wf, X, Y, Leq)$
⟨1⟩7. $\wedge\ W \subseteq Y$

$\land\ Wf = Floors(W,\ X,\ Leq)$
BY *UnfloorSetProperties*
⟨1⟩8. $W \subseteq Z \land Wf \subseteq Z$
BY ⟨1⟩1, ⟨1⟩7
⟨1⟩9. $\land\ IsFiniteSet(W)$
$\land\ Card(W) \leq Card(Wf)$
BY ⟨1⟩6, *ImageOfFinite* DEF *Unfloors*
⟨1⟩10. $CostLeq[\langle C,\ W\rangle]$
⟨2⟩ $\land\ W \in$ SUBSET Y
$\land\ IsACover(W,\ X,\ Leq)$
$\land\ CostLeq[\langle W,\ C\rangle]$
⟨3⟩ $IsACover(W,\ X,\ Leq)$
⟨4⟩ $IsUnfloor(W,\ Wf,\ X,\ Leq)$
BY ⟨1⟩7, ⟨1⟩9 DEF *IsUnfloor*
⟨4⟩ QED
BY ⟨1⟩7, ⟨1⟩5, *FloorPreservesCover*
⟨3⟩ $CostLeq[\langle W,\ C\rangle]$
⟨4⟩ $Card(W) \leq Card(C)$
BY ⟨1⟩9, ⟨1⟩6, ⟨1⟩2, *FS_CardinalityType*
⟨4⟩ QED
BY ⟨1⟩7 DEF *CardinalityAsCost*, *CostLeq*
⟨3⟩ QED
BY ⟨1⟩7
⟨2⟩ QED
BY ⟨1⟩3
⟨1⟩ $IsFiniteSet(W) \land IsFiniteSet(Wf) \land IsFiniteSet(Cf)$
BY ⟨1⟩9, ⟨1⟩2, ⟨1⟩6
⟨1⟩ USE *FS_CardinalityType* DEF *CardinalityAsCost*, *CostLeq*
⟨1⟩11. $Card(C) \leq Card(W)$
⟨2⟩ $C \subseteq Z \land W \subseteq Z$
BY ⟨1⟩8
⟨2⟩ QED
BY ⟨1⟩10
⟨1⟩12. $Card(Wf) < Card(Cf)$
⟨2⟩ $Cf \subseteq Z \land Wf \subseteq Z$
BY ⟨1⟩8, ⟨1⟩1
⟨2⟩ QED
BY ⟨1⟩5
⟨1⟩13. $Card(W) < Card(C)$
BY ⟨1⟩2, ⟨1⟩12, ⟨1⟩9
⟨1⟩ QED
BY ⟨1⟩11, ⟨1⟩13

LEMMA *UnfloorPreservesMinCover* $\triangleq$

ASSUME
NEW Leq, NEW X, NEW Y, NEW Cf, NEW C,
LET
$Z \triangleq Support(Leq)$
$Yf \triangleq Floors(Y, X, Leq)$
IN
$\land\ IsACompleteLattice(Leq)$
$\land\ CardinalityAsCost(Z)$
$\land\ X \subseteq Z$
$\land\ Y \subseteq Z \land IsFiniteSet(Y)$
$\land\ C \subseteq Y$
$\land\ IsAMinCover(Cf, X, Yf, Leq)$
Relation of unfloor C to Cf
$\land\ Cf = Floors(C, X, Leq)$
$\land\ Cardinality(C) \leq Cardinality(Cf)$
PROVE
$IsAMinCover(C, X, Y, Leq)$
PROOF
⟨1⟩ DEFINE
$Z \triangleq Support(Leq)$
$Yf \triangleq Floors(Y, X, Leq)$
$Card(S) \triangleq Cardinality(S)$
⟨1⟩1. $\land\ Yf \subseteq Z$
$\land\ IsFiniteSet(Yf)$
BY $FloorsIsSubset$, $FloorsSmaller$
⟨1⟩2. $\land\ IsACover(Cf, X, Leq)$
$\land\ Cf \in$ SUBSET Yf
$\land\ \forall\, r \in$ SUBSET Yf :
$\land\ IsACover(r, X, Leq)$
$\land\ CostLeq[\langle r, Cf\rangle]$
$\Rightarrow\ CostLeq[\langle Cf, r\rangle]$
BY $MinCoverProperties$
⟨1⟩3. SUFFICES ASSUME $\neg IsAMinCover(C, X, Y, Leq)$
PROVE FALSE
OBVIOUS
⟨1⟩4. PICK $W \in$ SUBSET Y :
$\land\ IsACover(W, X, Leq)$
$\land\ CostLeq[\langle W, C\rangle]$
$\land\ \neg CostLeq[\langle C, W\rangle]$
⟨2⟩ $C \in CoversOf(X, Y, Leq)$
⟨3⟩ $IsACover(C, X, Leq)$
BY ⟨1⟩2, $FloorPreservesCover$
⟨3⟩ $C \in$ SUBSET Y
OBVIOUS
⟨3⟩ QED

BY DEF *CoversOf*
⟨2⟩ QED
BY ⟨1⟩3, *CheaperCoverExists*
⟨1⟩ DEFINE $Wf \triangleq Floors(W, X, Leq)$
⟨1⟩5. $Wf \subseteq Yf$
BY ⟨1⟩4 DEF *Floors*
⟨1⟩6. $IsACover(Wf, X, Leq)$
BY ⟨1⟩4, *FloorPreservesCover*
⟨1⟩7. $W \subseteq Z \land Wf \subseteq Z \land Cf \subseteq Z$
BY ⟨1⟩5, ⟨1⟩4, ⟨1⟩2, ⟨1⟩1
⟨1⟩ $\land IsFiniteSet(W) \land IsFiniteSet(Wf)$
$\land IsFiniteSet(C) \land IsFiniteSet(Cf)$
BY ⟨1⟩4, ⟨1⟩2, ⟨1⟩1, *FS_Subset*, *FloorsSmaller*
⟨1⟩ $W \subseteq Z \land Wf \subseteq Z \land Cf \subseteq Z$
BY ⟨1⟩4, ⟨1⟩5, ⟨1⟩1, ⟨1⟩2
⟨1⟩ USE *FS_CardinalityType* DEF *CardinalityAsCost*, *CostLeq*
⟨1⟩8. $Card(C) \leq Card(W)$
⟨2⟩1. $Card(Wf) \leq Card(W)$
BY *FloorsSmaller*
⟨2⟩2. $CostLeq[\langle Wf, Cf \rangle]$
BY ⟨1⟩4, ⟨2⟩1
⟨2⟩3. $CostLeq[\langle Cf, Wf \rangle]$
BY ⟨1⟩2, ⟨1⟩5, ⟨1⟩6, ⟨2⟩2
⟨2⟩4. $Card(Cf) \leq Card(Wf)$
BY ⟨2⟩3
⟨2⟩ QED
BY ⟨2⟩4, ⟨2⟩1
⟨1⟩9. $Card(W) < Card(C)$
BY ⟨1⟩4
⟨1⟩ QED
BY ⟨1⟩8, ⟨1⟩9

FloorPreservesMinCover and UnfloorPreservesMinCover combined.
THEOREM *MinCoverPreservedIfFloors* $\triangleq$
ASSUME
NEW *Leq*, NEW *X*, NEW *Y*, NEW *C*, NEW *Cf*,
LET
$Z \triangleq Support(Leq)$
IN
$\land IsACompleteLattice(Leq)$
$\land CardinalityAsCost(Z)$
$\land X \subseteq Z$
$\land Y \subseteq Z \land IsFiniteSet(Y)$
$\land C \subseteq Y$

$\land\ Cf = Floors(C,\ X,\ Leq)$
$\land\ Cardinality(C) \leq Cardinality(Cf)$

PROVE

LET

$Yf \triangleq Floors(Y,\ X,\ Leq)$

IN

$\land\ IsAMinCover(C,\ X,\ Y,\ Leq) \equiv IsAMinCover(Cf,\ X,\ Yf,\ Leq)$
$\land\ Cardinality(C) = Cardinality(Cf)$

PROOF

$\langle 1\rangle$ DEFINE
$Yf \triangleq Floors(Y,\ X,\ Leq)$

$\langle 1\rangle 1.\ IsFiniteSet(C) \land IsFiniteSet(Cf)$
$\langle 2\rangle 1.\ (C \subseteq Y) \land IsFiniteSet(Y)$
OBVIOUS
$\langle 2\rangle 2.\ IsFiniteSet(C)$
BY $\langle 2\rangle 1$, *FS_Subset*
$\langle 2\rangle 3.\ Cf = Floors(C,\ X,\ Leq)$
OBVIOUS
$\langle 2\rangle 4.\ IsFiniteSet(Cf)$
BY $\langle 2\rangle 2$, $\langle 2\rangle 3$, *ImageOfFinite* DEF *Floors*
$\langle 2\rangle$ QED
BY $\langle 2\rangle 2$, $\langle 2\rangle 4$

$\langle 1\rangle 2.\ \land Cardinality(C) \in Nat$
$\land Cardinality(Cf) \in Nat$
BY $\langle 1\rangle 1$, *FS_CardinalityType*

$\langle 1\rangle 3.$ ASSUME $IsAMinCover(C,\ X,\ Y,\ Leq)$
PROVE $IsAMinCover(Cf,\ X,\ Yf,\ Leq)$
BY $\langle 1\rangle 3$, *FloorPreservesMinCover* DEF Yf

$\langle 1\rangle 4.$ ASSUME $IsAMinCover(Cf,\ X,\ Yf,\ Leq)$
PROVE $IsAMinCover(C,\ X,\ Y,\ Leq)$
BY $\langle 1\rangle 4$, *UnfloorPreservesMinCover* DEF Yf

$\langle 1\rangle 5.\ Cardinality(C) = Cardinality(Cf)$
$\langle 2\rangle$ DEFINE
$k \triangleq Cardinality(C)$
$m \triangleq Cardinality(Cf)$
$\langle 2\rangle 1.\ k \leq m$
BY DEF k, m
$\langle 2\rangle 2.\ m \leq k$
BY $\langle 1\rangle 1$, *ImageOfFinite* DEF k, m, *Floors*
$\langle 2\rangle 3.\ (k \in Nat) \land (m \in Nat)$
BY $\langle 1\rangle 2$
$\langle 2\rangle$ HIDE DEF k, m
$\langle 2\rangle 4.$ ASSUME
$(k \leq m) \land (m \leq k)$
PROVE $k = m$

BY $\langle 2\rangle 3$, $\langle 2\rangle 4$

$\langle 2\rangle$ QED

BY $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 4$ DEF k, m

$\langle 1\rangle$ QED

BY $\langle 1\rangle 3$, $\langle 1\rangle 4$, $\langle 1\rangle 5$

($*$ *Proofs checked with TLAPS version* 1.4.3 $*$)

MODULE *Orthotopes*

Definitions of discrete orthotopic covers.

Author: *Ioannis Filippidis*

EXTENDS
FiniteSets,
Reals

CONSTANTS $Variables$, $Domain$, $CareSet$

ASSUME $IsFiniteSet(Variables)$

$N \triangleq Cardinality(Variables)$
$Assignments \triangleq [Variables \to Int]$
ASSUME
$\land\ Domain \subseteq Assignments$
$\land\ Domain \neq \{\}$
$\land\ IsFiniteSet(Domain)$
$\land\ CareSet \subseteq Domain$

$Point \triangleq Domain \cap CareSet$

$EndPoint(k) \triangleq [1 \,..\, k \to Assignments]$
$IsInOrthotope(x,\ a,\ b) \triangleq \forall\, var \in Variables :$
$\quad (a[var] \leq x[var]) \land (x[var] \leq b[var])$
$IsNonEmpty(a,\ b) \triangleq \exists\, x \in Assignments :\ IsInOrthotope(x,\ a,\ b)$
$IsInRegion(x,\ p,\ q) \triangleq \exists\, i \in \text{DOMAIN } p \ :\ IsInOrthotope(x,\ p[i],\ q[i])$
$OrthotopicSet(a,\ b) \triangleq \{x \in Assignments :\ IsInOrthotope(x,\ a,\ b)\}$
$Orthotope(Dom) \triangleq \{OrthotopicSet(a,\ b) :\ a,\ b \in Dom\}$
$SameOver(f,\ p,\ q,\ S) \triangleq \forall\, x \in S :\ f[x] \equiv IsInRegion(x,\ p,\ q)$

CONSTANT f
p, q define a cover that contains k orthotopes
$IsMinDNF(k,\ p,\ q) \triangleq$
$\land\ SameOver(f,\ p,\ q,\ Point)$
$\land\ \forall\, r \in Nat :\ \forall\, u,\ v \in EndPoint(r) :$ u, v define a cover that contains r orthotopes
$\lor\ \neg SameOver(f,\ u,\ v,\ Point)$ not a cover, or
$\lor\ r \geq k$ u, v has at least as many disjuncts as p, q

Problem: Minimal orthotopic formula in disjunctive normal form for *BDD*.
Assumptions about the characteristic function f to cover.
ASSUME
$\land\ f \in [Assignments \to \text{BOOLEAN }]$

$\wedge\, \forall\, x \in \mathit{Assignments} \setminus \mathit{CareSet} :\ f[x] = \text{FALSE}$

THEOREM

$\exists\, k \in \mathit{Nat} :\ \exists\, p,\ q \in \mathit{EndPoint}(k) :\ \mathit{IsMinDNF}(k,\ p,\ q)$

PROOF OMITTED some *DNF* exists, by finiteness of *CareSet*

MODULE *CyclicCore*

Correctness of the cyclic core computation.

This algorithm was originally proposed in [1].

Author: Ioannis *Filippidis*

References

[1] *Olivier Coudert* "Two-level logic minimization: An overview" Integration, the *VLSI* Journal Vol.17, No.2, *Oct* 1994, pp. 97–140 10.1016/0167 − 9260(94)00007 − 7

EXTENDS
FiniteSetFacts,
Integers,
Lattices,
MinCover,
Optimization,
TLAPS

CONSTANTS
Leq,
Xinit, *Yinit*

VARIABLES
X, Current set to be covered.
Y, Set of elements available for covering *X*.
E, Accumulates essential elements.
Xold, *Yold*, History variables used to detect fixpoint.
i Program counter.

$Z \triangleq Support(Leq)$
ASSUMPTION $CostIsCard \triangleq$
$Cost = [cover \in \text{SUBSET } Z \mapsto Cardinality(cover)]$

Definitions for convenience.
$RowRed(u, v) \triangleq MaxCeilings(u, v, Leq)$
$ColRed(u, v) \triangleq MaxFloors(v, u, Leq)$

$Card(S) \triangleq Cardinality(S)$ shorthand

$InitIsFeasible \triangleq \exists C : IsACoverFrom(C, Xinit, Yinit, Leq)$

ASSUMPTION $ProblemInput \triangleq$
$\land IsACompleteLattice(Leq)$
$\land IsFiniteSet(Z)$
$\land Xinit \subseteq Z$
$\land Yinit \subseteq Z$
$\land InitIsFeasible$

THEOREM $HaveCardAsCost \triangleq CardinalityAsCost(Z)$
PROOF
BY $CostIsCard$ DEF $CardinalityAsCost$

THEOREM $LeqTransitive \triangleq IsTransitive(Leq)$
PROOF
BY $ProblemInput$ DEF $IsACompleteLattice$, $IsACompleteLattice$, $IsAPartialOrder$

THEOREM $LeqIsPor \triangleq IsAPartialOrder(Leq)$
PROOF
BY $ProblemInput$ DEF $IsACompleteLattice$

Specification of cyclic core computation.

$TypeInv \triangleq$
$\land X \in \text{SUBSET } Z$
$\land Y \in \text{SUBSET } Z$
$\land E \in \text{SUBSET } Z$
$\land Xold \in \text{SUBSET } Z$
$\land Yold \in \text{SUBSET } Z$
$\land i \in 1 \,..\, 3$

$Init \triangleq$
$\land X = Xinit$
$\land Y = Yinit$
$\land E = \{\}$
$\land Xold = \{\}$
$\land Yold = \{\}$
$\land i = 1$

$ReduceColumns \triangleq$
$\land (i = 1) \land (i' = 2)$
$\land Y' = ColRed(X, Y)$
$\land Xold' = X$
$\land Yold' = Y$
$\land \text{UNCHANGED } \langle X, E \rangle$

$ReduceRows \triangleq$
$\land (i = 2) \land (i' = 3)$
$\land X' = RowRed(X, Y)$
$\land$ UNCHANGED $\langle Y, E, Xold, Yold \rangle$

$RemoveEssential \triangleq$
$\land (i = 3) \land (i' = 1)$
$\land$ LET
$Ess \triangleq X \cap Y$ Essential elements.
IN
$\land X' = X \setminus Ess$
$\land Y' = Y \setminus Ess$
$\land E' = E \cup Ess$
$\land$ UNCHANGED $\langle Xold, Yold \rangle$

$Next \triangleq$
$\lor ReduceColumns$
$\lor ReduceRows$
$\lor RemoveEssential$

$vars \triangleq \langle X, Y, E, Xold, Yold, i \rangle$
$Spec \triangleq Init \land \Box[Next]_{vars} \land \mathrm{WF}_{vars}(Next)$

$IsFeasible \triangleq \exists C : IsAMinCover(C, X, Y, Leq)$
$HatIsMinCover \triangleq$
$\forall C, H :$
$\lor \neg \land IsAMinCover(C, X, Y, Leq)$
$\land IsAHat(H, C \cup E, Yinit, Leq)$
$\lor \land IsAMinCover(H, Xinit, Yinit, Leq)$
$\land Cardinality(H) = Cardinality(C) + Cardinality(E)$

$Useful \triangleq \Box(IsFeasible \land HatIsMinCover)$
$ReachesFixpoint \triangleq \Diamond\Box[\text{FALSE}]_{\langle X, Y \rangle}$

Invariants.

THEOREM $TypeOK \triangleq Spec \Rightarrow \Box TypeInv$
PROOF
$\langle 1 \rangle 1.$ ASSUME $Init$
PROVE $TypeInv$
$\langle 2 \rangle 1. \{\} \in$ SUBSET Z
OBVIOUS
$\langle 2 \rangle 2. \land X = Xinit \land Y = Yinit \land i = 1$
$\land E = \{\} \land Xold = \{\} \land Yold = \{\}$

BY $\langle 1\rangle 1$ DEF *Init*

$\langle 2\rangle 3$. $Xinit \in \text{SUBSET } Z \land Yinit \in \text{SUBSET } Z$

BY *ProblemInput*

$\langle 2\rangle 4$. $X \in \text{SUBSET } Z \land Y \in \text{SUBSET } Z$

BY $\langle 2\rangle 2$, $\langle 2\rangle 3$

$\langle 2\rangle 5$. $\land E \in \text{SUBSET } Z$
$\land Xold \in \text{SUBSET } Z \land Yold \in \text{SUBSET } Z$

BY $\langle 2\rangle 1$, $\langle 2\rangle 2$

$\langle 2\rangle 6$. $i \in 1 \,..\, 3$

BY $\langle 2\rangle 2$

$\langle 2\rangle$ QED

BY $\langle 2\rangle 4$, $\langle 2\rangle 5$, $\langle 2\rangle 6$ DEF *TypeInv*

$\langle 1\rangle 2$. ASSUME $TypeInv \land Next$
PROVE $TypeInv'$

$\langle 2\rangle 4$. $\land X \in \text{SUBSET } Z \land Y \in \text{SUBSET } Z$
$\land E \in \text{SUBSET } Z$
$\land Xold \in \text{SUBSET } Z \land Yold \in \text{SUBSET } Z$
$\land i \in 1 \,..\, 3$

BY $\langle 1\rangle 2$ DEF *TypeInv*

$\langle 2\rangle 1$. ASSUME *ReduceColumns*
PROVE $TypeInv'$

$\langle 3\rangle 2$. $\land (i = 1) \land (i' = 2)$
$\land Y' = ColRed(X, Y)$
$\land Xold' = X$
$\land Yold' = Y$
$\land \text{UNCHANGED } \langle X, E\rangle$

BY $\langle 2\rangle 1$ DEF *ReduceColumns*

$\langle 3\rangle 3$. $i' \in 1 \,..\, 3$

BY $\langle 3\rangle 2$

$\langle 3\rangle 4$. $Xold' \in \text{SUBSET } Z \land Yold' \in \text{SUBSET } Z$

BY $\langle 3\rangle 2$, $\langle 2\rangle 4$

$\langle 3\rangle 5$. $X' \in \text{SUBSET } Z \land E' \in \text{SUBSET } Z$

BY $\langle 3\rangle 2$, $\langle 2\rangle 4$

$\langle 3\rangle 6$. $Y' = MaxFloors(Y, X, Leq)$

BY $\langle 3\rangle 2$ DEF *ColRed*

$\langle 3\rangle 7$. $Y' \in \text{SUBSET } Z$

BY $\langle 3\rangle 6$, $\langle 2\rangle 4$, *FloorsIsSubset*, *MaxIsSubset*, *ProblemInput*
DEF *MaxFloors*, *Z*

$\langle 3\rangle$ QED

BY $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$, $\langle 3\rangle 7$ DEF *TypeInv*

$\langle 2\rangle 2$. ASSUME $TypeInv \land ReduceRows$
PROVE $TypeInv'$

$\langle 3\rangle 1$. $\land (i = 2) \land (i' = 3)$
$\land X' = RowRed(X, Y)$
$\land \text{UNCHANGED } \langle Y, E, Xold, Yold\rangle$

BY $\langle 2\rangle 2$ DEF *ReduceRows*

$\langle 3\rangle 2$. $i' \in 1 \,..\, 3$

BY $\langle 3\rangle 1$

$\langle 3\rangle 3$. $\land\ Y' \in \text{SUBSET}\ Z \land E' \in \text{SUBSET}\ Z$
$\land\ Xold' \in \text{SUBSET}\ Z \land Yold' \in \text{SUBSET}\ Z$

BY $\langle 3\rangle 1$, $\langle 2\rangle 4$

$\langle 3\rangle 4$. $X' = MaxCeilings(X,\ Y,\ Leq)$

BY $\langle 3\rangle 1$ DEF *RowRed*

$\langle 3\rangle 5$. $X' \in \text{SUBSET}\ Z$

BY $\langle 3\rangle 4$, $\langle 2\rangle 4$, *CeilingsIsSubset*, *MaxIsSubset*, *ProblemInput*
DEF *MaxCeilings*, *Z*

$\langle 3\rangle$ QED

BY $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 5$ DEF *TypeInv*

$\langle 2\rangle 3$. ASSUME *TypeInv* $\land$ *RemoveEssential*
PROVE *TypeInv*$'$

$\langle 3\rangle$ DEFINE
Ess $\triangleq\ X \cap Y$

$\langle 3\rangle 1$. $\land\ (i\ = 3) \land (i' = 1)$
$\land\ X' = X \setminus Ess$
$\land\ Y' = Y \setminus Ess$
$\land\ E' = E \cup Ess$
$\land$ UNCHANGED $\langle Xold,\ Yold\rangle$

BY $\langle 2\rangle 3$ DEF *RemoveEssential*

$\langle 3\rangle 2$. $i' \in 1 \,..\, 3$

BY $\langle 3\rangle 1$

$\langle 3\rangle 3$. $Xold' \in \text{SUBSET}\ Z \land Yold' \in \text{SUBSET}\ Z$

BY $\langle 3\rangle 1$, $\langle 2\rangle 4$

$\langle 3\rangle 4$. $X' \in \text{SUBSET}\ Z \land Y' \in \text{SUBSET}\ Z$

$\langle 4\rangle 1$. $X' \subseteq X \land Y' \subseteq Y$

BY $\langle 3\rangle 1$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 2\rangle 4$

$\langle 3\rangle 5$. $E' \in \text{SUBSET}\ Z$

$\langle 4\rangle 1$. $Ess \in \text{SUBSET}\ Z$

$\langle 5\rangle 1$. $Ess \subseteq X$

BY $\langle 3\rangle 1$

$\langle 5\rangle 2$. $X \in \text{SUBSET}\ Z$

BY $\langle 2\rangle 4$

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle 2$. $E' = E \cup Ess$

BY $\langle 3\rangle 1$

$\langle 4\rangle 3$. $E \in \text{SUBSET}\ Z$

BY $\langle 2\rangle 4$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 1$

$\langle 3\rangle$ QED

BY $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$ DEF *TypeInv*

$\langle 2\rangle$ QED

BY $\langle 1\rangle 2$, $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$ DEF *Next*

$\langle 1\rangle 3$. ASSUME $TypeInv \wedge [Next]_{vars}$

PROVE $TypeInv'$

BY $\langle 1\rangle 2$, $\langle 1\rangle 3$ DEF *Next*, *vars*, *TypeInv*

$\langle 1\rangle$ QED

$\langle 2\rangle$ DEFINE

$Inv \triangleq TypeInv$

$Nx \triangleq Next$

$\langle 2\rangle 1$. ASSUME $Inv \wedge [Nx]_{vars}$

PROVE Inv'

BY $\langle 2\rangle 1$, $\langle 1\rangle 3$ DEF *Inv*, *Nx*

$\langle 2\rangle 2$. $(TypeInv \wedge \Box[Next]_{vars}) \Rightarrow \Box\, TypeInv$

BY $\langle 2\rangle 1$, *PTL* DEF *Inv*, *Nx*

$\langle 2\rangle 3$. $(Init \wedge \Box[Next]_{vars}) \Rightarrow \Box\, TypeInv$

BY $\langle 1\rangle 1$, $\langle 2\rangle 2$

$\langle 2\rangle$ QED

BY $\langle 2\rangle 3$ DEF *Spec*

THEOREM $MaximalAtEssAux \triangleq$

$$Spec \Rightarrow \Box \wedge (i = 2) \Rightarrow \begin{array}{l} \wedge\ X = Xold \\ \wedge\ Y = ColRed(Xold,\ Yold) \end{array}$$

$$\wedge (i = 3) \Rightarrow \begin{array}{l} \wedge\ X = RowRed(Xold,\ Y) \\ \wedge\ Y = ColRed(Xold,\ Yold) \end{array}$$

PROOF

$\langle 1\rangle$ DEFINE $Inv \triangleq$

$$\wedge (i = 2) \Rightarrow \begin{array}{l} \wedge\ X = Xold \\ \wedge\ Y = ColRed(Xold,\ Yold) \end{array}$$

$$\wedge (i = 3) \Rightarrow \begin{array}{l} \wedge\ X = RowRed(Xold,\ Y) \\ \wedge\ Y = ColRed(Xold,\ Yold) \end{array}$$

$\langle 1\rangle 1$. ASSUME *Init*

PROVE *Inv*

BY $\langle 1\rangle 1$ DEF *Init*, *Inv*

$\langle 1\rangle 2$. ASSUME $Inv \wedge [Next]_{vars}$

PROVE Inv'

$\langle 2\rangle 1$. SUFFICES ASSUME *Next*

PROVE Inv'

BY $\langle 1\rangle 2$, $\langle 2\rangle 1$ DEF *vars*

$\langle 2\rangle 2$. ASSUME *ReduceColumns*

PROVE Inv'

BY $\langle 2\rangle 2$ DEF *ReduceColumns*, *Inv*

⟨2⟩3. ASSUME *ReduceRows*
PROVE *Inv*′
BY ⟨1⟩2, ⟨2⟩3 DEF *ReduceRows*, *Inv*
⟨2⟩4. ASSUME *RemoveEssential*
PROVE *Inv*′
BY ⟨1⟩2, ⟨2⟩4 DEF *RemoveEssential*, *Inv*
⟨2⟩ QED goal from ⟨2⟩1
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4 DEF *Next*
⟨1⟩ QED
⟨2⟩1. $(Inv \wedge \Box[Next]_{vars}) \Rightarrow \Box Inv$
BY ⟨1⟩2, *PTL*
⟨2⟩2. $(Init \wedge \Box[Next]_{vars}) \Rightarrow \Box Inv$
BY ⟨2⟩1, ⟨1⟩1
⟨2⟩ QED
BY ⟨2⟩2, *PTL* DEF *Spec*

THEOREM $MaximalAtEss \triangleq$
$Spec \Rightarrow \Box \vee i \neq 3$
$\vee \wedge X = RowRed(Xold,\ Y)$
$\wedge Y = ColRed(Xold,\ Yold)$
PROOF
⟨1⟩ DEFINE
$InvMaxAtEss \triangleq$
$\wedge (i = 2) \Rightarrow \wedge X = Xold$
$\wedge Y = ColRed(Xold,\ Yold)$
$\wedge \vee i \neq 3$
$\vee \wedge X = RowRed(Xold,\ Y)$
$\wedge Y = ColRed(Xold,\ Yold)$
⟨1⟩2. $(\ \wedge (i = 2) \Rightarrow \wedge X = Xold$
$\wedge Y = ColRed(Xold,\ Yold)$
$\wedge (i\ \ = 3) \Rightarrow \wedge X = RowRed(Xold,\ Y)$
$\wedge Y = ColRed(Xold,\ Yold)) \Rightarrow InvMaxAtEss$
OBVIOUS
⟨1⟩ QED
BY ⟨1⟩2, *MaximalAtEssAux*, *PTL*

More invariants.

THEOREM $Spec \Rightarrow \Box(X \subseteq Z \wedge Y \subseteq Z)$
PROOF
⟨1⟩ DEFINE $Inv \triangleq \wedge X \subseteq Z$
$\wedge Y \subseteq Z$
⟨1⟩1. ASSUME *TypeInv*

PROVE Inv
BY $\langle 1\rangle 1$ DEF $TypeInv$, Inv
$\langle 1\rangle 2$. $(\Box TypeInv) \Rightarrow \Box Inv$
BY $\langle 1\rangle 1$, PTL
$\langle 1\rangle$ QED
BY $TypeOK$, $\langle 1\rangle 2$, PTL

THEOREM $YERefinesYinit \triangleq$
$Spec \Rightarrow \Box Refines(Y \cup E,\ Yinit,\ Leq)$
PROOF
$\langle 1\rangle$ DEFINE
$Inv \triangleq Refines(Y \cup E,\ Yinit,\ Leq)$
$\langle 1\rangle 1$. $Spec \Rightarrow \Box(IsFiniteSet(X) \land IsFiniteSet(Y))$
$\langle 2\rangle 1$. $Spec \Rightarrow \Box TypeInv$
BY $TypeOK$
$\langle 2\rangle 2$. $(\Box TypeInv) \Rightarrow \Box(IsFiniteSet(X) \land IsFiniteSet(Y))$
$\langle 3\rangle 1$. $TypeInv \Rightarrow \land X \in$ SUBSET Z
$\land Y \in$ SUBSET Z
BY DEF $TypeInv$
$\langle 3\rangle 2$. $IsFiniteSet(Z)$
BY $ProblemInput$
$\langle 3\rangle 3$. $TypeInv \Rightarrow (IsFiniteSet(X) \land IsFiniteSet(Y))$
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, FS_Subset
$\langle 3\rangle$ QED
BY $\langle 3\rangle 3$, PTL
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$
$\langle 1\rangle 2$. $Inv' = Refines(Y' \cup E',\ Yinit,\ Leq)$
BY DEF Inv, $Refines$
$\langle 1\rangle 3$. ASSUME $TypeInv \land Inv \land ReduceColumns$
PROVE Inv'
$\langle 2\rangle 1$. SUFFICES $Refines(Y' \cup E',\ Yinit,\ Leq)$
BY $\langle 1\rangle 2$
$\langle 2\rangle 2$. SUFFICES
ASSUME NEW $u \in (Y' \cup E')$
PROVE $\exists\, v \in Yinit :\ Leq[u,\ v]$
BY $\langle 2\rangle 1$ DEF $Refines$, $Refines$ goal from $\langle 2\rangle 1$
$\langle 2\rangle 3$. ASSUME NEW $w \in (Y \cup E)$
PROVE $\exists\, v \in Yinit :\ Leq[w,\ v]$
$\langle 3\rangle 1$. $Refines(Y \cup E,\ Yinit,\ Leq)$
BY $\langle 1\rangle 3$ DEF Inv
$\langle 3\rangle$ QED
BY $\langle 3\rangle 1$ DEF $Refines$, $Refines$
$\langle 2\rangle 4$. CASE $u \in E'$

⟨3⟩1. $E' = E$
BY ⟨1⟩3 DEF *ReduceColumns*
⟨3⟩2. $u \in E$
BY ⟨2⟩2, ⟨2⟩4, ⟨2⟩3, ⟨3⟩1
⟨3⟩ QED goal from ⟨2⟩2
BY ⟨3⟩2, ⟨2⟩3
⟨2⟩5. CASE $u \in Y'$
⟨3⟩1. $Y' = MaxFloors(Y, X, Leq)$
BY ⟨1⟩3 DEF *ReduceColumns*, *ColRed*
⟨3⟩2. $Y' \subseteq Floors(Y, X, Leq)$
BY ⟨3⟩1, *MaxIsSubset* DEF *MaxFloors*
⟨3⟩3. $u \in Floors(Y, X, Leq)$
BY ⟨2⟩5, ⟨3⟩2
⟨3⟩4. PICK $y \in Y : u = Floor(y, X, Leq)$
BY ⟨3⟩3 DEF *Floors*
⟨3⟩8. $y \in Z$
BY ⟨3⟩4, ⟨1⟩3 DEF *TypeInv*
⟨3⟩5. $Leq[u, y]$
⟨4⟩2. $X \subseteq Z$
BY ⟨1⟩3 DEF *TypeInv*
⟨4⟩3. $Z = Support(Leq)$
BY DEF Z
⟨4⟩4. $IsACompleteLattice(Leq)$
BY *ProblemInput*
⟨4⟩ QED
BY ⟨3⟩8, ⟨4⟩2, ⟨4⟩3, ⟨4⟩4, *FloorIsSmaller*, ⟨3⟩4
⟨3⟩6. PICK $v \in Yinit : Leq[y, v]$
BY ⟨2⟩3, ⟨3⟩4
⟨3⟩7. $u \in Z$
BY ⟨3⟩3, *FloorsIsSubset*, *ProblemInput*, ⟨1⟩3 DEF *TypeInv*, Z
⟨3⟩11. $v \in Z$
BY ⟨3⟩6, *ProblemInput*
⟨3⟩9. $Leq[u, y] \land Leq[y, v]$
BY ⟨3⟩5, ⟨3⟩6
⟨3⟩10. $Leq[u, v]$
BY ⟨3⟩8, ⟨3⟩7, ⟨3⟩11, ⟨3⟩9, *ProblemInput*, *LeqTransitive*
DEF *IsTransitive*, Z
⟨3⟩ QED
⟨4⟩1. $v \in Yinit$
BY ⟨3⟩6
⟨4⟩ QED goal from ⟨2⟩2
BY ⟨3⟩10, ⟨4⟩1
⟨2⟩ QED
BY ⟨2⟩4, ⟨2⟩5, ⟨2⟩2 exhaustive by ⟨2⟩2
⟨1⟩4. ASSUME $Inv \land RemoveEssential$

PROVE Inv'
⟨2⟩ DEFINE $Ess \triangleq X \cap Y$
⟨2⟩1. $\wedge\ Y' = Y \setminus Ess$
$\wedge\ E' = E \cup Ess$
BY ⟨1⟩4 DEF *RemoveEssential*
⟨2⟩2. $(Y' \cup E') = (Y \cup E)$
⟨3⟩1. $(Y' \cup E') = ((Y \setminus Ess) \cup (E \cup Ess))$
BY ⟨2⟩1
⟨3⟩2. $(Y' \cup E') = ((Ess \cup (Y \setminus Ess)) \cup E)$
BY ⟨3⟩1
⟨3⟩3. $(Ess \cup (Y \setminus Ess)) = Y$
⟨4⟩1. $Y \subseteq (Ess \cup (Y \setminus Ess))$
OBVIOUS
⟨4⟩2. $Ess \subseteq Y$
BY DEF Ess
⟨4⟩3. $(Ess \cup (Y \setminus Ess)) \subseteq Y$
BY ⟨4⟩2
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩3
⟨3⟩ QED
BY ⟨3⟩2, ⟨3⟩3
⟨2⟩3. $Refines(Y \cup E,\ Yinit,\ Leq)$
BY ⟨1⟩4 DEF Inv
⟨2⟩4. $Refines(Y' \cup E',\ Yinit,\ Leq)$
BY ⟨2⟩3, ⟨2⟩2
⟨2⟩ QED
BY ⟨2⟩4, ⟨1⟩2
⟨1⟩5. ASSUME $Inv \wedge ReduceRows$
PROVE Inv'
⟨2⟩1. $(Y' \cup E') = (Y \cup E)$
⟨3⟩1. $Y' = Y \wedge E' = E$
BY ⟨1⟩5 DEF *ReduceRows*
⟨3⟩ QED
BY ⟨3⟩1
⟨2⟩2. $Refines(Y \cup E,\ Yinit,\ Leq)$
BY ⟨1⟩5 DEF Inv
⟨2⟩3. $Refines(Y' \cup E',\ Yinit,\ Leq)$
BY ⟨2⟩1, ⟨2⟩2
⟨2⟩ QED
BY ⟨2⟩3, ⟨1⟩2
⟨1⟩6. ASSUME $TypeInv \wedge Inv \wedge Next$
PROVE Inv'
BY ⟨1⟩6, ⟨1⟩3, ⟨1⟩4, ⟨1⟩5 DEF $Next$
⟨1⟩7. ASSUME $Init$
PROVE Inv

⟨2⟩1. SUFFICES $Refines(Y \cup E,\ Yinit,\ Leq)$
BY DEF Inv
⟨2⟩2. $Y = Yinit \land E = \{\}$
BY ⟨1⟩7 DEF $Init$
⟨2⟩3. $(Y \cup E) = Yinit$
BY ⟨2⟩2
⟨2⟩4. $Refines(Yinit,\ Yinit,\ Leq)$
⟨3⟩1. $\forall\, u \in Yinit :\ Leq[u,\ u]$
⟨4⟩1. $Yinit \subseteq Z$
BY *ProblemInput*
⟨4⟩2. $IsACompleteLattice(Leq) \land Z = Support(Leq)$
BY *ProblemInput* DEF Z
⟨4⟩3. $\forall\, u \in Z :\ Leq[u,\ u]$
BY ⟨4⟩2 DEF *IsACompleteLattice*, *IsACompleteLattice*, *IsAPartialOrder*, *IsAPartialOrder*, *IsReflexive*
⟨4⟩ QED
BY ⟨4⟩3, ⟨4⟩1
⟨3⟩2. $\forall\, u \in Yinit :\ \exists\, v \in Yinit :\ Leq[u,\ u]$
BY ⟨3⟩1
⟨3⟩ QED
BY ⟨3⟩2 DEF *Refines*
⟨2⟩ QED goal from ⟨2⟩1
BY ⟨2⟩3, ⟨2⟩4
⟨1⟩ HIDE DEF Inv
⟨1⟩8. ASSUME $Inv \land [TypeInv \land Next]_{vars}$
PROVE Inv'
BY ⟨1⟩8, ⟨1⟩6 DEF Inv, $vars$
⟨1⟩ QED
⟨2⟩1. $(Inv \land \Box[TypeInv \land Next]_{vars}) \Rightarrow \Box Inv$
BY ⟨1⟩8, *PTL*
⟨2⟩2. $(Init \land \Box[TypeInv \land Next]_{vars}) \Rightarrow \Box Inv$
BY ⟨2⟩1, ⟨1⟩7
⟨2⟩3. $(Init \land \Box\, TypeInv \land \Box[Next]_{vars}) \Rightarrow \Box Inv$
BY ⟨2⟩2, *PTL*
⟨2⟩ QED
BY ⟨2⟩3, *TypeOK* DEF *Spec*, *Inv*

THEOREM $XinitRefinesXE \triangleq$
$Spec \Rightarrow \Box Refines(Xinit,\ X \cup E,\ Leq)$
PROOF
⟨1⟩ DEFINE $Inv \triangleq Refines(Xinit,\ X \cup E,\ Leq)$
⟨1⟩1. ASSUME $Init$
PROVE Inv

⟨2⟩1. ∧ $X = Xinit$
∧ $E = \{\}$
BY ⟨1⟩1 DEF *Init*
⟨2⟩2. *Refines*($Xinit$, $Xinit$, *Leq*)
⟨3⟩1. SUFFICES ASSUME NEW $u \in Xinit$
PROVE *Leq*[u, u]
BY ⟨3⟩1 DEF *Refines*
⟨3⟩2. SUFFICES $u \in Support(Leq)$
BY ⟨3⟩2, *LeqIsPor* DEF *IsAPartialOrder*, *IsReflexive*
⟨3⟩ QED goal from ⟨3⟩2
BY *ProblemInput*, ⟨3⟩1 DEF *Z*
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2
⟨1⟩2. ASSUME $Inv \land [TypeInv \land TypeInv' \land Next]_{vars}$
PROVE Inv'
⟨2⟩1. SUFFICES ASSUME $TypeInv \land TypeInv' \land Next$
PROVE Inv'
BY ⟨1⟩2, ⟨2⟩1 DEF *vars*
⟨2⟩2. ASSUME *ReduceColumns*
PROVE Inv'
BY ⟨1⟩2, ⟨2⟩2 DEF *ReduceColumns*
⟨2⟩3. ASSUME *ReduceRows*
PROVE Inv'
⟨3⟩1. SUFFICES
ASSUME NEW $u \in Xinit$
PROVE $\exists\, v \in (X' \cup E') :$ *Leq*[u, v]
BY ⟨3⟩1 DEF *Refines*
⟨3⟩2. PICK $r \in (X \cup E) :$ *Leq*[u, r]
BY ⟨1⟩2, ⟨3⟩1 DEF *Refines*
⟨3⟩3.CASE $r \in E$
BY ⟨3⟩2, ⟨3⟩3, ⟨2⟩3 DEF *ReduceRows*
⟨3⟩4.CASE $r \in X$
⟨4⟩2. ∧ $u \in Z$
∧ $r \in Z$
BY ⟨2⟩1, ⟨3⟩1, ⟨3⟩4, *ProblemInput* DEF *TypeInv*
⟨4⟩1. PICK $v \in X' :$ *Leq*[r, v]
⟨5⟩ DEFINE
$t \triangleq Ceil(r, Y, Leq)$
$S \triangleq Ceilings(X, Y, Leq)$
⟨5⟩1. ∧ $t \in S$
∧ *Leq*[r, t]
⟨6⟩1. $t \in S$
BY ⟨3⟩4 DEF t, *Ceilings*
⟨6⟩2. *Leq*[r, t]
BY ⟨2⟩1, ⟨3⟩4, *ProblemInput*,

CeilIsLarger DEF *TypeInv*, *Z*

⟨6⟩ QED
BY ⟨6⟩1, ⟨6⟩2

⟨5⟩2. $X' = Maxima(S, Leq)$
BY ⟨2⟩3 DEF *ReduceRows*, *RowRed*, *MaxCeilings*

⟨5⟩6. $S \subseteq Z$
BY ⟨2⟩1, *CeilingsIsSubset*, *ProblemInput*
DEF *TypeInv*, *Z*

⟨5⟩3. PICK $v \in X' : Leq[t, v]$

⟨6⟩1. PICK $v \in S : \land Leq[t, v]$
$\land IsMaximal(v, S, Leq)$
BY ⟨5⟩1, ⟨5⟩6, *HasSomeMaximalAbove*, *ProblemInput*
DEF *IsACompleteLattice*, *IsAPartialOrder*, *Z*

⟨6⟩2. $v \in X'$
BY ⟨5⟩2, ⟨6⟩1 DEF *Maxima*

⟨6⟩ QED
BY ⟨6⟩1, ⟨6⟩2

⟨5⟩5. $\land r \in Z$
$\land t \in Z$
$\land v \in Z$
BY ⟨4⟩2, ⟨5⟩1, ⟨5⟩6, ⟨5⟩3, ⟨2⟩1,
ProblemInput DEF *TypeInv*

⟨5⟩ QED
BY ⟨5⟩3, ⟨5⟩1, ⟨5⟩5, *LeqTransitive*
DEF *IsTransitive*, *Z*

⟨4⟩3. $v \in Z$
BY ⟨2⟩1, ⟨4⟩1, *ProblemInput* DEF *TypeInv*

⟨4⟩ QED
BY ⟨3⟩2, ⟨4⟩1, ⟨4⟩2, ⟨4⟩3, *LeqTransitive*
DEF *IsTransitive*, *Z*

⟨3⟩ QED
BY ⟨3⟩3, ⟨3⟩4, ⟨2⟩3 DEF *ReduceRows*

⟨2⟩4. ASSUME *RemoveEssential*
PROVE Inv'

⟨3⟩ DEFINE $Ess \triangleq X \cap Y$

⟨3⟩1. $\land X' = X \setminus Ess$
$\land E' = E \cup Ess$
BY ⟨2⟩4 DEF *RemoveEssential*

⟨3⟩2. $(X' \cup E') = (X \cup E)$
BY ⟨3⟩1

⟨3⟩ QED
BY ⟨1⟩2, ⟨3⟩2

⟨2⟩ QED goal from ⟨2⟩1
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4 DEF *Next*

⟨1⟩ QED

$\langle 2\rangle 1.\ (Inv \land \Box[TypeInv \land TypeInv' \land Next]_{vars}) \ \Rightarrow\ \Box Inv$
BY $\langle 1\rangle 2,\ PTL$
$\langle 2\rangle 2.\ (Init \land \Box[TypeInv \land TypeInv' \land Next]_{vars}) \ \Rightarrow\ \Box Inv$
BY $\langle 2\rangle 1,\ \langle 1\rangle 1$
$\langle 2\rangle 3.\ (Init \land \Box TypeInv \land \Box[Next]_{vars}) \ \Rightarrow\ \Box Inv$
BY $\langle 2\rangle 2,\ PTL$
$\langle 2\rangle$ QED
BY $\langle 2\rangle 3,\ TypeOK,\ PTL$ DEF $Spec$

THEOREM $YincompE \triangleq$
$Spec \Rightarrow \Box(\forall\, y \in Y :\ \forall\, e \in E :\ \neg Leq[e,\ y])$
PROOF
$\langle 1\rangle$ DEFINE
$Inv \triangleq \forall\, y \in Y :\ \forall\, e \in E :\ \neg Leq[e,\ y]$
$Aux \triangleq \lor\ i \neq 3$
$\lor\ \land X = RowRed(Xold,\ Y)$
$\land\ Y = ColRed(Xold,\ Yold)$
$\langle 1\rangle$ HIDE DEF $Inv,\ Aux$
$\langle 1\rangle 1.$ ASSUME $Init$
PROVE Inv
$\langle 2\rangle 1.\ E = \{\}$
BY $\langle 1\rangle 1$ DEF $Init$
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1$ DEF Inv
$\langle 1\rangle 2.$ ASSUME $\land\ TypeInv \land Inv \land Next$
$\land\ \lor\ i \neq 3$
$\lor\ \land X = RowRed(Xold,\ Y)$
$\land\ Y = ColRed(Xold,\ Yold)$
PROVE Inv'
$\langle 2\rangle 1.$ ASSUME $Inv \land ReduceColumns$
PROVE Inv'
$\langle 3\rangle 1.\ \land\ Y' = MaxFloors(Y,\ X,\ Leq)$
$\land\ E' = E$
BY $\langle 2\rangle 1$ DEF $ReduceColumns,\ ColRed$
$\langle 3\rangle 2.$ SUFFICES
ASSUME NEW $y \in Y'$, NEW $e \in E'$
PROVE $\neg Leq[e,\ y]$
BY DEF Inv
$\langle 3\rangle 3.$ SUFFICES
ASSUME $Leq[e,\ y]$
PROVE FALSE
OBVIOUS goal from $\langle 3\rangle 2$
$\langle 3\rangle 4.\ e \in E$
BY $\langle 3\rangle 2,\ \langle 3\rangle 1$

⟨3⟩5. $Y' = Maxima(Floors(Y, X, Leq), Leq)$
BY ⟨3⟩1 DEF $Maxima$, $Maxima$, $MaxFloors$
⟨3⟩6. $Y' \subseteq Floors(Y, X, Leq)$
BY ⟨3⟩5, $MaxIsSubset$
⟨3⟩7. PICK $p \in Y : y = Floor(p, X, Leq)$
BY ⟨3⟩2, ⟨3⟩6 DEF $Floors$
⟨3⟩14. $p \in Z$
⟨4⟩1. $Y \in$ SUBSET Z
BY ⟨1⟩2 DEF $TypeInv$
⟨4⟩ QED
BY ⟨3⟩7, ⟨4⟩1
⟨3⟩8. $Leq[y, p]$
⟨4⟩1. $X \subseteq Z$
BY ⟨1⟩2 DEF $TypeInv$
⟨4⟩2. $Z = Support(Leq)$
BY DEF Z
⟨4⟩3. $IsACompleteLattice(Leq)$
BY $ProblemInput$
⟨4⟩ QED
BY ⟨3⟩7, ⟨3⟩14, ⟨4⟩1, ⟨4⟩2, ⟨4⟩3, $FloorIsSmaller$
⟨3⟩12. $Leq[e, p]$
⟨4⟩1. $Leq[e, y] \land Leq[y, p]$
BY ⟨3⟩3, ⟨3⟩8
⟨4⟩2. $(e \in Z) \land (y \in Z) \land (p \in Z)$
⟨5⟩1. $e \in Z$
⟨6⟩1. $E \in$ SUBSET Z
BY ⟨1⟩2 DEF $TypeInv$
⟨6⟩ QED
BY ⟨3⟩4, ⟨6⟩1
⟨5⟩2. $y \in Z$
⟨6⟩1. $y = Floor(p, X, Leq)$
BY ⟨3⟩7
⟨6⟩2. $IsACompleteLattice(Leq)$
BY $ProblemInput$
⟨6⟩3. $X \subseteq Z$
BY ⟨1⟩2 DEF $TypeInv$
⟨6⟩4. $Z = Support(Leq)$
BY DEF Z
⟨6⟩ QED
BY ⟨6⟩1, ⟨6⟩2, ⟨6⟩3, ⟨6⟩4, $FloorExists$
⟨5⟩ QED
BY ⟨5⟩1, ⟨5⟩2, ⟨3⟩14
⟨4⟩3. $IsTransitive(Leq)$
BY $ProblemInput$ DEF $IsACompleteLattice$, $IsACompleteLattice$, $IsAPartialOrder$

⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3 DEF *IsTransitive*, *Z*
⟨3⟩13. $\neg Leq[e,\ p]$
⟨4⟩1. $(p \in Y) \land (e \in E)$
BY ⟨3⟩4, ⟨3⟩7
⟨4⟩ QED
BY ⟨4⟩1, ⟨1⟩2 DEF *Inv*
⟨3⟩ QED
BY ⟨3⟩12, ⟨3⟩13
⟨2⟩2. ASSUME $Inv \land ReduceRows$
PROVE Inv'
⟨3⟩1. $(Y' = Y) \land (E' = E)$
BY ⟨2⟩2 DEF *ReduceRows*
⟨3⟩2. $\forall\, y \in Y :\ \forall\, e \in E :\ \neg Leq[e,\ y]$
BY ⟨2⟩2 DEF *Inv*
⟨3⟩3. $\forall\, y \in Y' :\ \forall\, e \in E' :\ \neg Leq[e,\ y]$
BY ⟨3⟩1, ⟨3⟩2
⟨3⟩ QED
BY ⟨3⟩3 DEF *Inv*
⟨2⟩3. ASSUME $Inv \land RemoveEssential$
PROVE Inv'
⟨3⟩ DEFINE $Ess \triangleq X \cap Y$
⟨3⟩1. $(Y' = (Y \setminus Ess)) \land (E' = (E \cup Ess))$
BY ⟨2⟩3 DEF *RemoveEssential*
⟨3⟩2. $\forall\, y \in Y :\ \forall\, e \in E :\ \neg Leq[e,\ y]$
BY ⟨2⟩3 DEF *Inv*
⟨3⟩3. SUFFICES
ASSUME NEW $y \in Y'$, NEW $e \in E'$
PROVE $\neg Leq[e,\ y]$
BY DEF *Inv*
⟨3⟩4. $Y' \subseteq Y$
BY ⟨3⟩1
⟨3⟩5. $y \in Y$
BY ⟨3⟩3, ⟨3⟩4
⟨3⟩6. $(e \in E) \lor (e \in Ess)$
BY ⟨3⟩1, ⟨3⟩3
⟨3⟩7. CASE $e \in E$
BY ⟨3⟩5, ⟨3⟩7, ⟨3⟩2
⟨3⟩8. CASE $e \in Ess$
⟨4⟩1. $\forall\, p,\ q \in Y :\ (p \neq q) \Rightarrow \neg Leq[p,\ q]$
⟨5⟩1. $\exists\, S :\ Y = Maxima(S,\ Leq)$
BY ⟨1⟩2, ⟨2⟩3 DEF *ColRed*, *MaxFloors*, *RemoveEssential*
⟨5⟩2. $Y = Maxima(Y,\ Leq)$
BY ⟨5⟩1, *MaxIsIdempotent*
⟨5⟩3. $Y \subseteq Support(Leq)$

⟨6⟩1. $Y \in \text{SUBSET } Z$
BY ⟨1⟩2 DEF *TypeInv*
⟨6⟩2. $Z = Support(Leq)$
BY DEF Z
⟨6⟩ QED
BY ⟨6⟩1, ⟨6⟩2
⟨5⟩4. *IsAntiSymmetric*(*Leq*)
BY *ProblemInput* DEF *IsACompleteLattice*, *IsACompleteLattice*, *IsAPartialOrder*
⟨5⟩5. *IsAntiChain*(*Y*, *Leq*)
BY ⟨5⟩2, ⟨5⟩3, ⟨5⟩4, *MaximaIsAntiChain*
⟨5⟩ QED
BY ⟨5⟩5 DEF *IsAntiChain*
⟨4⟩2. $e \neq y$
⟨5⟩1. $y \in (Y \setminus Ess)$
BY ⟨3⟩3, ⟨3⟩1
⟨5⟩2. $y \notin Ess$
BY ⟨5⟩1
⟨5⟩3. $e \in Ess$
BY ⟨3⟩8
⟨5⟩ QED
BY ⟨5⟩2, ⟨5⟩3
⟨4⟩3. $(e \in Y) \land (y \in Y)$
BY ⟨3⟩8, ⟨3⟩5 DEF *Ess*
⟨4⟩ QED goal from ⟨3⟩3
BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3
⟨3⟩ QED
BY ⟨3⟩7, ⟨3⟩8, ⟨3⟩6
⟨2⟩ QED
BY ⟨1⟩2, ⟨2⟩1, ⟨2⟩2, ⟨2⟩3 DEF *Next*
⟨1⟩3. ASSUME $Inv \land [TypeInv \land Aux \land Next]_{vars}$
PROVE Inv'
BY ⟨1⟩3, ⟨1⟩2 DEF *Inv*, *Aux*, *vars*
⟨1⟩ QED
⟨2⟩1. $(Inv \land \Box[TypeInv \land Aux \land Next]_{vars}) \Rightarrow \Box Inv$
BY ⟨1⟩3, *PTL*
⟨2⟩2. $(Init \land \Box[TypeInv \land Aux \land Next]_{vars}) \Rightarrow \Box Inv$
BY ⟨2⟩1, ⟨1⟩1
⟨2⟩3. $(Init \land \Box TypeInv \land \Box Aux \land \Box[Next]_{vars}) \Rightarrow \Box Inv$
BY ⟨2⟩2, *PTL*
⟨2⟩ QED
BY ⟨2⟩3, *PTL*, *MaximalAtEss*, *TypeOK* DEF *Spec*, *Aux*, *Inv*

THEOREM *noYcapE* $\triangleq$

$Spec \Rightarrow \Box((Y \cap E) = \{\})$

PROOF

$\langle 1 \rangle 1$. $Spec \Rightarrow \Box(TypeInv \land (\forall\, y \in Y :\ \forall\, e \in E :\ \neg Leq[e,\, y]))$

BY $TypeOK$, $YincompE$

$\langle 1 \rangle 7$. SUFFICES

ASSUME $TypeInv \land (\forall\, y \in Y :\ \forall\, e \in E :\ \neg Leq[e,\, y])$

PROVE $(Y \cap E) = \{\}$

BY $\langle 1 \rangle 1$, $\langle 1 \rangle 7$, PTL

$\langle 1 \rangle 2$. SUFFICES

ASSUME NEW $y \in (Y \cap E)$,

$\land \quad TypeInv$

$\land \quad \forall\, q \in Y :\ \forall\, e \in E :\ \neg Leq[e,\, q]$

PROVE FALSE

BY $\langle 1 \rangle 7$, $\langle 1 \rangle 2$

$\langle 1 \rangle 3$. $\neg Leq[y,\, y]$

BY $\langle 1 \rangle 2$

$\langle 1 \rangle 4$. $IsReflexive(Leq)$

BY $ProblemInput$ DEF $IsACompleteLattice$, $IsACompleteLattice$, $IsAPartialOrder$

$\langle 1 \rangle 5$. $y \in Support(Leq)$

$\langle 2 \rangle 1$. $y \in Y$

BY $\langle 1 \rangle 2$

$\langle 2 \rangle 2$. $Y \subseteq Z$

BY $\langle 1 \rangle 2$ DEF $TypeInv$

$\langle 2 \rangle 3$. $Z = Support(Leq)$

BY DEF Z

$\langle 2 \rangle$ QED

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

$\langle 1 \rangle 6$. $Leq[y,\, y]$

BY $\langle 1 \rangle 5$, $\langle 1 \rangle 4$ DEF $IsReflexive$

$\langle 1 \rangle$ QED goal from $\langle 1 \rangle 2$

BY $\langle 1 \rangle 3$, $\langle 1 \rangle 6$

A minimal cover of $Xinit$, $Yinit$ can be constructed from a minimal cover of X, Y.

THEOREM $HatIsMinCoverInit \triangleq$

ASSUME $Init$

PROVE $HatIsMinCover$

PROOF

$\langle 1 \rangle 1$. SUFFICES

ASSUME

NEW C, NEW H,

$\land\, IsAMinCover(C,\, X,\, Y,\, Leq)$

$\land\, IsAHat(H,\, C \cup E,\, Yinit,\, Leq)$

PROVE
$\land\ IsAMinCover(H,\ Xinit,\ Yinit,\ Leq)$
$\land\ Card(H) = Card(C) + Card(E)$
BY $\langle 1\rangle 1$ DEF $HatIsMinCover,\ Card$
$\langle 1\rangle 2.\ \land\ E = \{\}$
$\land\ X = Xinit$
$\land\ Y = Yinit$
BY DEF $Init$
$\langle 1\rangle 3.\ \land\ (C \cup E) = C$
$\land\ Card(C) + Card(E) = Card(C)$
$\langle 2\rangle 1.\ (C \cup E) = C$
BY $\langle 1\rangle 2$
$\langle 2\rangle 2.\ Card(C) + Card(E) = Card(C)$
$\langle 3\rangle 1.\ Card(C) \in Nat$
BY $\langle 1\rangle 1,\ \langle 1\rangle 2,\ MinCoverProperties,\ ProblemInput,\ FS\_Subset,$
$FS\_CardinalityType$ DEF $Card$
$\langle 3\rangle 2.\ Card(E) = 0$
BY $\langle 1\rangle 2,\ FS\_EmptySet$ DEF $Card$
$\langle 3\rangle$ QED
BY $\langle 3\rangle 1,\ \langle 3\rangle 2$
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1,\ \langle 2\rangle 2$
$\langle 1\rangle 4.\ IsAHat(H,\ C,\ Yinit,\ Leq)$
BY $\langle 1\rangle 1,\ \langle 1\rangle 3$
$\langle 1\rangle 5.\ IsAMinCover(H,\ X,\ Y,\ Leq)$
$\langle 2\rangle 1.\ \land\ H \in$ SUBSET Y
$\land\ Cardinality(H) \leq Cardinality(C)$
BY $\langle 1\rangle 4,\ \langle 1\rangle 2$ DEF $IsAHat$
$\langle 2\rangle 2.\ IsACover(H,\ X,\ Leq)$
$\langle 3\rangle 1.\ Refines(X,\ C,\ Leq)$
BY $\langle 1\rangle 1,\ MinCoverProperties,\ RefinesMeansCover$
$\langle 3\rangle 2.\ Refines(C,\ H,\ Leq)$
BY $\langle 1\rangle 4,\ \langle 1\rangle 2$ DEF $IsAHat$
$\langle 3\rangle 3.\ \land\ X \subseteq Z$
$\land\ C \subseteq Z$
$\land\ H \subseteq Z$
BY $\langle 2\rangle 1,\ \langle 1\rangle 2,\ ProblemInput,\ \langle 1\rangle 1,\ MinCoverProperties$
$\langle 3\rangle$ QED
BY $\langle 3\rangle 1,\ \langle 3\rangle 2,\ \langle 3\rangle 3,\ RefinesIsTransitive,$
$LeqTransitive,\ RefinesMeansCover$ DEF Z
$\langle 2\rangle$ QED
BY $\langle 1\rangle 1,\ \langle 2\rangle 1,\ \langle 2\rangle 2,\ HaveCardAsCost,$
$MinCoverEquivCoverCard,\ \langle 1\rangle 2,\ ProblemInput,\ FS\_Subset$
$\langle 1\rangle 6.\ Card(H) = Card(C) + Card(E)$
$\langle 2\rangle 1.\ Card(H) = Card(C)$

⟨3⟩1. $IsAMinCover(C,\ X,\ Y,\ Leq)$
BY ⟨1⟩1
⟨3⟩2. $\land\ Y \in \text{SUBSET}\ Z$
$\land\ IsFiniteSet(Y)$
BY ⟨1⟩2, *ProblemInput*, *FS_Subset*
⟨3⟩3. $CardinalityAsCost(Z)$
BY *ProblemInput*, *HaveCardAsCost*
⟨3⟩ QED
BY ⟨1⟩5, ⟨3⟩1, ⟨3⟩2, ⟨3⟩3,
AllMinCoversSameCard DEF *Card*
⟨2⟩ QED
BY ⟨2⟩1, ⟨1⟩3
⟨1⟩ QED
BY ⟨1⟩5, ⟨1⟩6 DEF *Init*

THEOREM $HatIsMinCoverUnchangedByReduceColumns \triangleq$
ASSUME
$\land\ TypeInv \land TypeInv'$
$\land\ ((Y \cap E) = \{\})'$
$\land\ Refines(Xinit,\ X \cup E,\ Leq)$
$\land\ Refines(Y \cup E,\ Yinit,\ Leq)$
$\land\ HatIsMinCover$
$\land\ ReduceColumns$
PROVE
$HatIsMinCover'$
PROOF
⟨1⟩1. $IsFiniteSet(Xinit) \land IsFiniteSet(Yinit)$
⟨2⟩1. $Xinit \subseteq Z \land Yinit \subseteq Z$
BY *ProblemInput*
⟨2⟩2. $IsFiniteSet(Z)$
BY *ProblemInput*
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, *FS_Subset*
⟨1⟩2. $IsFiniteSet(X) \land IsFiniteSet(Y)$
⟨2⟩1. $X \in \text{SUBSET}\ Z \land Y \in \text{SUBSET}\ Z$
BY DEF *TypeInv*
⟨2⟩2. $IsFiniteSet(Z)$
BY *ProblemInput*
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, *FS_Subset*
⟨1⟩3. SUFFICES
ASSUME NEW C, NEW H,
$\land\quad IsAMinCover(C,\ X',\ Y',\ Leq)$
$\land\quad IsAHat(H,\ C \cup E',\ Yinit,\ Leq)$

PROVE
$\land\ IsAMinCover(H,\ Xinit,\ Yinit,\ Leq)$
$\land\ Card(H) = Card(C) + Card(E')$
BY DEF $HatIsMinCover,\ Card$
$\langle 1\rangle 4.\ E' = E \land X' = X$
BY DEF $ReduceColumns$
$\langle 1\rangle 5.\ H \subseteq Z$
$\langle 2\rangle 1.\ H \subseteq Yinit$
BY $\langle 1\rangle 3$ DEF $IsAHat$
$\langle 2\rangle 2.\ Yinit \subseteq Z$
BY $ProblemInput$
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1,\ \langle 2\rangle 2$
$\langle 1\rangle 6.\ X \in$ SUBSET $Z \land E \in$ SUBSET Z
BY DEF $TypeInv$
$\langle 1\rangle 7.\ \land\ IsAMinCover(C,\ X,\ Y',\ Leq)$
$\land\ IsAHat(H,\ C \cup E,\ Yinit,\ Leq)$
BY $\langle 1\rangle 3,\ \langle 1\rangle 4$
$\langle 1\rangle 8.\ IsACoverFrom(H,\ Xinit,\ Yinit,\ Leq)$
$\langle 2\rangle 2.\ IsACover(C,\ X,\ Leq)$
BY $\langle 1\rangle 7,\ MinCoverProperties$
$\langle 2\rangle 3.\ IsACover(C \cup E,\ X \cup E,\ Leq)$
$\langle 3\rangle 1.\ \forall\, x \in X :\ \exists\, y \in C :\ Leq[x,\ y]$
BY $\langle 2\rangle 2$ DEF $IsACover$
$\langle 3\rangle 2.$ SUFFICES
ASSUME NEW $x \in (X \cup E)$
PROVE $\exists\, y \in (C \cup E) :\ Leq[x,\ y]$
BY DEF $IsACover$
$\langle 3\rangle 3.$CASE $x \in X$
$\langle 4\rangle 1.$ PICK $y \in C :\ Leq[x,\ y]$
BY $\langle 3\rangle 1,\ \langle 3\rangle 3$
$\langle 4\rangle 2.\ y \in (C \cup E)$
BY $\langle 4\rangle 1$
$\langle 4\rangle$ QED goal from $\langle 3\rangle 2$
BY $\langle 4\rangle 1,\ \langle 4\rangle 2$
$\langle 3\rangle 4.$CASE $x \in E$
$\langle 4\rangle 1.\ x \in Z$
$\langle 5\rangle 1.\ E \in$ SUBSET Z
BY DEF $TypeInv$
$\langle 5\rangle$ QED
BY $\langle 3\rangle 4,\ \langle 5\rangle 1$
$\langle 4\rangle 2.\ IsReflexive(Leq)$
BY $ProblemInput$ DEF $IsACompleteLattice,$
$IsAPartialOrder$
$\langle 4\rangle 3.\ Leq[x,\ x]$

BY ⟨4⟩1, ⟨4⟩2 DEF *IsReflexive*, *Z*

⟨4⟩4. $x \in (C \cup E)$

BY ⟨3⟩4

⟨4⟩ QED

BY ⟨4⟩3, ⟨4⟩4

⟨3⟩ QED

BY ⟨3⟩3, ⟨3⟩4, ⟨3⟩2

⟨2⟩4. *IsACover*$(H, X \cup E, Leq)$

⟨3⟩1. $\forall\, u \in (X \cup E) : \exists\, v \in (C \cup E) : Leq[u, v]$

BY ⟨2⟩3 DEF *IsACover*

⟨3⟩2. *Refines*$(C \cup E, H, Leq)$

BY ⟨1⟩7 DEF *IsAHat*

⟨3⟩3. $\forall\, p \in (C \cup E) : \exists\, q \in H : Leq[p, q]$

BY ⟨3⟩2 DEF *Refines*

⟨3⟩4. SUFFICES

ASSUME NEW $u \in (X \cup E)$

PROVE $\exists\, y \in H : Leq[u, y]$

BY DEF *IsACover*

⟨3⟩5. PICK $v \in (C \cup E) : Leq[u, v]$

BY ⟨3⟩4, ⟨3⟩1

⟨3⟩6. PICK $q \in H : Leq[v, q]$

BY ⟨3⟩5, ⟨3⟩3

⟨3⟩7. $Leq[u, v] \land Leq[v, q]$

BY ⟨3⟩5, ⟨3⟩6

⟨3⟩8. $(u \in Z) \land (v \in Z) \land (q \in Z)$

⟨4⟩1. $u \in Z$

⟨5⟩2. $u \in (X \cup E)$

BY ⟨3⟩4

⟨5⟩ QED

BY ⟨1⟩6, ⟨5⟩2

⟨4⟩2. $v \in Z$

⟨5⟩1. $v \in (C \cup E)$

BY ⟨3⟩5

⟨5⟩2. $E \in$ SUBSET Z

BY DEF *TypeInv*

⟨5⟩3. $Y' \in$ SUBSET Z

BY DEF *TypeInv*

⟨5⟩4. $C \in$ SUBSET Y'

BY ⟨1⟩3, *MinCoverProperties*

⟨5⟩5. $C \in$ SUBSET Z

BY ⟨5⟩3, ⟨5⟩4

⟨5⟩6. $(C \cup E) \in$ SUBSET Z

BY ⟨5⟩2, ⟨5⟩5

⟨5⟩ QED

BY ⟨5⟩1, ⟨5⟩6

⟨4⟩3. $q \in Z$
⟨5⟩1. $q \in H$
BY ⟨3⟩6
⟨5⟩ QED
BY ⟨5⟩1, ⟨1⟩5
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3
⟨3⟩9. $Leq[u,\ q]$
BY ⟨3⟩7, ⟨3⟩8, *LeqTransitive* DEF *IsTransitive*, Z
⟨3⟩ QED
⟨4⟩1. $Leq[u,\ q] \land (q \in H)$
BY ⟨3⟩9, ⟨3⟩6
⟨4⟩ QED goal from ⟨3⟩4
BY ⟨4⟩1
⟨2⟩5. $Refines(Xinit,\ X \cup E,\ Leq)$
OBVIOUS
⟨2⟩6. $IsACover(H,\ Xinit,\ Leq)$ *TODO*
⟨3⟩1. $H \subseteq Z$
BY ⟨1⟩5
⟨3⟩2. $Xinit \subseteq Z$
BY *ProblemInput*
⟨3⟩3. $(X \cup E) \subseteq Z$
BY ⟨1⟩6
⟨3⟩4. $\land\ IsACover(X \cup E,\ Xinit,\ Leq)$
$\land\ IsACover(H,\ X \cup E,\ Leq)$
BY ⟨2⟩4, ⟨2⟩5, *RefinesMeansCover*
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, *LeqTransitive*, *CoveringIsTransitive* DEF Z
⟨2⟩ QED
⟨3⟩1. $IsAHat(H,\ C \cup E,\ Yinit,\ Leq) \Rightarrow (H \subseteq Yinit)$
BY DEF *IsAHat*
⟨3⟩2. $H \subseteq Yinit$
BY ⟨3⟩1, ⟨1⟩7
⟨3⟩ QED
BY ⟨2⟩6, ⟨3⟩2 DEF *IsACoverFrom*
⟨1⟩ DEFINE $H2 \triangleq Hat(C,\ Y,\ Leq)$
⟨1⟩9. $\land\ C \subseteq MaxFloors(Y,\ X,\ Leq)$
$\land\ C \subseteq Z$
⟨2⟩1. $C \subseteq Y'$
BY ⟨1⟩3, *MinCoverProperties*
⟨2⟩2. $Y' = MaxFloors(Y,\ X,\ Leq)$
⟨3⟩1. $Y' = ColRed(X,\ Y)$
BY DEF *ReduceColumns*
⟨3⟩ QED

BY $\langle 3\rangle 1$ DEF *ColRed*

$\langle 2\rangle 3$. $Y' \in$ SUBSET Z

BY DEF *TypeInv*

$\langle 2\rangle$ QED

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

$\langle 1\rangle 10$. $IsFiniteSet(C)$

$\langle 3\rangle 1$. $IsFiniteSet(Z)$

BY *ProblemInput*

$\langle 3\rangle 2$. $C \subseteq Z$

BY $\langle 1\rangle 9$

$\langle 3\rangle$ QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, *FS_Subset*

$\langle 1\rangle 11$. $\wedge\ C = Floors(H2,\ X,\ Leq)$
$\wedge\ C \subseteq MaxFloors(Y,\ X,\ Leq)$
$\wedge\ Card(C) = Card(H2)$

$\langle 2\rangle 1$. $X \in$ SUBSET $Z \wedge Y \in$ SUBSET Z

BY DEF *TypeInv*

$\langle 2\rangle 2$. $C \subseteq MaxFloors(Y,\ X,\ Leq)$

BY $\langle 1\rangle 9$

$\langle 2\rangle 4$. $IsACompleteLattice(Leq)$

BY *ProblemInput*

$\langle 2\rangle$ QED

BY $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 1\rangle 10$, $\langle 2\rangle 4$,
MaxFloorsHatIsUnfloor DEF $H2$, Z, *Card*

$\langle 1\rangle$ DEFINE

$Yf \triangleq Floors(Y,\ X,\ Leq)$

$\langle 1\rangle 12$. $H2 \subseteq Y$

$\langle 2\rangle 1$. SUFFICES

ASSUME NEW $u \in C$

PROVE $\exists\, r \in Y :\ Leq[u,\ r]$

BY DEF $H2$, *Hat*, *SomeAbove*

$\langle 2\rangle 2$. $C \subseteq MaxFloors(Y,\ X,\ Leq)$

BY $\langle 1\rangle 11$

$\langle 2\rangle 3$. $C \subseteq Maxima(Floors(Y,\ X,\ Leq),\ Leq)$

BY $\langle 2\rangle 2$ DEF *MaxFloors*

$\langle 2\rangle 4$. $C \subseteq Floors(Y,\ X,\ Leq)$

BY $\langle 2\rangle 3$ DEF *Maxima*

$\langle 2\rangle 5$. $u \in Floors(Y,\ X,\ Leq)$

BY $\langle 2\rangle 1$, $\langle 2\rangle 4$

$\langle 2\rangle 6$. PICK $r \in Y :\ u = Floor(r,\ X,\ Leq)$

BY $\langle 2\rangle 5$ DEF *Floors*

$\langle 2\rangle 7$. $r \in Z$

BY $\langle 2\rangle 6$ DEF *TypeInv*

$\langle 2\rangle 8$. $X \subseteq Z$

BY DEF *TypeInv*

⟨2⟩9. $\wedge$ $IsACompleteLattice(Leq)$
$\wedge$ $Z = Support(Leq)$
BY $ProblemInput$ DEF Z
⟨2⟩10. $Leq[u,\ r]$
BY ⟨2⟩6, ⟨2⟩7, ⟨2⟩8, ⟨2⟩9, $FloorIsSmaller$
⟨2⟩ QED goal from ⟨2⟩1
BY ⟨2⟩6, ⟨2⟩10
⟨1⟩13. $IsAMinCover(H2,\ X,\ Y,\ Leq)$
⟨2⟩1. $IsAMinCover(H2,\ X,\ Y,\ Leq) \equiv IsAMinCover(C,\ X,\ Yf,\ Leq)$
⟨3⟩1. $IsACompleteLattice(Leq)$
BY $ProblemInput$
⟨3⟩2. $CardinalityAsCost(Z)$
BY $HaveCardAsCost$
⟨3⟩3. $X \subseteq Z$
BY DEF $TypeInv$
⟨3⟩4. $Y \subseteq Z \wedge IsFiniteSet(Y)$
⟨4⟩1. $Y \in$ SUBSET Z
BY DEF $TypeInv$
⟨4⟩2. $IsFiniteSet(Z)$
BY $ProblemInput$
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2, FS_Subset
⟨3⟩5. $H2 \subseteq Y$
BY ⟨1⟩12
⟨3⟩6. $C = Floors(H2,\ X,\ Leq)$
BY ⟨1⟩11
⟨3⟩8. $Cardinality(H2) \leq Cardinality(C)$
⟨4⟩1. $Card(C) = Card(H2)$
BY ⟨1⟩11
⟨4⟩2. $IsFiniteSet(C)$
BY ⟨1⟩10
⟨4⟩3. $IsFiniteSet(H2)$
⟨5⟩1. $Y \in$ SUBSET Z
BY DEF $TypeInv$
⟨5⟩2. $IsFiniteSet(Z)$
BY $ProblemInput$
⟨5⟩3. $IsFiniteSet(Y)$
BY ⟨5⟩1, ⟨5⟩2, FS_Subset
⟨5⟩4. $H2 \subseteq Y$
BY ⟨1⟩12
⟨5⟩ QED
BY ⟨5⟩3, ⟨5⟩4, FS_Subset
⟨4⟩ QED BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3, $FS\_CardinalityType$ DEF $Card$
⟨3⟩9. $Z = Support(Leq)$
BY DEF Z

⟨3⟩10. $Yf = Floors(Y, X, Leq)$
BY DEF Yf
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩8, ⟨3⟩9, ⟨3⟩10, *MinCoverPreservedIfFloors*
⟨2⟩2. $IsAMinCover(C, X, Y', Leq)$
BY ⟨1⟩7
⟨2⟩5. $Y' = Maxima(Yf, Leq)$
⟨3⟩1. $Y' = MaxFloors(Y, X, Leq)$
BY DEF *ReduceColumns*, *ColRed*
⟨3⟩2. $Y' = Maxima(Floors(Y, X, Leq), Leq)$
BY ⟨3⟩1 DEF *MaxFloors*
⟨3⟩ QED
BY ⟨3⟩2 DEF Yf
⟨2⟩6. $IsAMinCover(C, X, Yf, Leq)$
⟨3⟩1. $X \subseteq Z \land Y \subseteq Z$
BY DEF *TypeInv*
⟨3⟩2. $Yf \subseteq Z$
⟨4⟩1. $Yf = Floors(Y, X, Leq)$
BY DEF Yf
⟨4⟩ QED
BY ⟨4⟩1, ⟨3⟩1, *ProblemInput*, *FloorsIsSubset* DEF Z
⟨3⟩ QED
BY ⟨2⟩2, ⟨2⟩5, ⟨3⟩1, ⟨3⟩2, *ProblemInput*, *LeqIsPor*, *HaveCardAsCost*, *MinCoversFromMaxSuffice* DEF Z
$Max \leftarrow Y'$, $Y \leftarrow Yf$
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩6
⟨1⟩14. ASSUME
NEW $Cnew$, NEW $Hnew$,
$\land\ IsAMinCover(Cnew, X, Y, Leq)$
$\land\ IsAHat(Hnew, Cnew \cup E, Yinit, Leq)$
PROVE
$\land\ IsAMinCover(Hnew, Xinit, Yinit, Leq)$
$\land\ Card(Hnew) = Card(Cnew) + Card(E)$
BY ⟨1⟩14 DEF *HatIsMinCover*, *Card*
⟨1⟩15. ASSUME
NEW $Hnew$,
$IsAHat(Hnew, H2 \cup E, Yinit, Leq)$
PROVE
$\land\ IsAMinCover(Hnew, Xinit, Yinit, Leq)$
$\land\ Card(Hnew) = Card(H2) + Card(E)$
BY ⟨1⟩13, ⟨1⟩14, ⟨1⟩15 $Cnew \leftarrow H2$
⟨1⟩16. PICK $H3 : IsAHat(H3, H2 \cup E, Yinit, Leq)$
⟨2⟩1. $H2 \subseteq Y$

BY $\langle 1\rangle 12$
$\langle 2\rangle 2.\ (H2 \cup E) \subseteq (Y \cup E)$
BY $\langle 2\rangle 1$
$\langle 2\rangle 3.\ \mathit{Refines}(Y \cup E,\ \mathit{Yinit},\ \mathit{Leq})$
OBVIOUS
$\langle 2\rangle 4.\ \mathit{Refines}(H2 \cup E,\ \mathit{Yinit},\ \mathit{Leq})$
BY $\langle 2\rangle 2$, $\langle 2\rangle 3$ DEF *Refines* can refine this proof
$\langle 2\rangle$ DEFINE
$W \triangleq \mathit{Hat}(H2 \cup E,\ \mathit{Yinit},\ \mathit{Leq})$
$\langle 2\rangle 6.\ \mathit{Card}(W) \leq \mathit{Card}(H2 \cup E)$
$\langle 3\rangle$ DEFINE $S \triangleq H2 \cup E$
$\langle 3\rangle 1.\ \mathit{IsFiniteSet}(S)$
$\langle 4\rangle 1.\ H2 \subseteq Y$
BY $\langle 1\rangle 12$
$\langle 4\rangle 2.\ Y \in \text{SUBSET } Z \land E \in \text{SUBSET } Z$
BY DEF *TypeInv*
$\langle 4\rangle 3.\ (H2 \cup E) \subseteq Z$
BY $\langle 4\rangle 1$, $\langle 4\rangle 2$
$\langle 4\rangle 4.\ \mathit{IsFiniteSet}(Z)$
BY *ProblemInput*
$\langle 4\rangle$ QED
BY $\langle 4\rangle 3$, $\langle 4\rangle 4$, *FS_Subset* DEF S
$\langle 3\rangle 2.\ W = \{\mathit{SomeAbove}(y,\ \mathit{Yinit},\ \mathit{Leq}) :\ y \in S\}$
BY DEF W, *Hat*, S
$\langle 3\rangle$ HIDE DEF $H2$, W, S
$\langle 3\rangle 3.\ \mathit{Cardinality}(\{\mathit{SomeAbove}(y,\ \mathit{Yinit},\ \mathit{Leq}) :\ y \in S\})$
$\leq \mathit{Cardinality}(S)$
BY $\langle 3\rangle 1$, *ImageOfFinite*
$\langle 3\rangle$ QED
BY $\langle 3\rangle 2$, $\langle 3\rangle 3$ DEF S, *Card*
$\langle 2\rangle 7.\ \mathit{IsAHat}(W,\ H2 \cup E,\ \mathit{Yinit},\ \mathit{Leq})$
$\langle 3\rangle 5.\ \forall\, u \in (H2 \cup E) :\ \exists\, y \in \mathit{Yinit} :\ \mathit{Leq}[u,\ y]$
BY $\langle 2\rangle 4$ DEF *Refines*
$\langle 3\rangle 4.\ \forall\, u \in (H2 \cup E) :\ \exists\, y \in \mathit{Yinit} :$
$\land\ y = \mathit{SomeAbove}(u,\ \mathit{Yinit},\ \mathit{Leq})$
$\land\ \mathit{Leq}[u,\ y]$
BY $\langle 3\rangle 5$ DEF *SomeAbove*
$\langle 3\rangle 1.\ W \subseteq \mathit{Yinit}$
$\langle 4\rangle 3.\ \forall\, y \in \mathit{Hat}(H2 \cup E,\ \mathit{Yinit},\ \mathit{Leq}) :\ y \in \mathit{Yinit}$
BY $\langle 3\rangle 4$ DEF *Hat*
$\langle 4\rangle 4.\ \forall\, y \in W :\ y \in \mathit{Yinit}$
BY $\langle 4\rangle 3$ DEF W
$\langle 4\rangle$ QED
BY $\langle 4\rangle 4$
$\langle 3\rangle 2.\ \mathit{Refines}(H2 \cup E,\ W,\ \mathit{Leq})$

⟨4⟩1. SUFFICES
ASSUME NEW $u \in (H2 \cup E)$
PROVE $\exists\, y \in W :\ Leq[u,\ y]$
BY DEF *Refines*
⟨4⟩2. PICK $y \in Yinit :\ \wedge\, y = SomeAbove(u,\ Yinit,\ Leq)$
$\wedge\, Leq[u,\ y]$
BY ⟨3⟩4
⟨4⟩3. $y \in W$
BY ⟨4⟩2 DEF W, *Hat*
⟨4⟩ QED goal from ⟨4⟩1
BY ⟨4⟩2, ⟨4⟩3
⟨3⟩3. $Card(W) \leq Card(H2 \cup E)$
BY ⟨2⟩6
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3 DEF *IsAHat*, *Card*
⟨2⟩ QED
BY ⟨2⟩7
⟨1⟩17. $\wedge\, IsAMinCover(H3,\ Xinit,\ Yinit,\ Leq)$
$\wedge\, Card(H3) = Card(H2) + Card(E)$
BY ⟨1⟩15, ⟨1⟩16
⟨1⟩18. $Card(H3) = Card(C) + Card(E)$
BY ⟨1⟩11, ⟨1⟩17
⟨1⟩19. $Card(H) \in Nat \wedge Card(H3) \in Nat$
⟨2⟩1. $IsFiniteSet(H) \wedge IsFiniteSet(H3)$
⟨3⟩1. $IsFiniteSet(H)$
⟨4⟩1. $H \subseteq Z$
BY ⟨1⟩5
⟨4⟩2. $IsFiniteSet(Z)$
BY *ProblemInput*
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2, *FS_Subset*
⟨3⟩2. $IsFiniteSet(H3)$
⟨4⟩1. $H3 \subseteq Yinit$
BY ⟨1⟩17, *MinCoverProperties*
⟨4⟩2. $IsFiniteSet(Yinit)$
⟨5⟩1. $(Yinit \in \text{SUBSET } Z) \wedge IsFiniteSet(Z)$
BY *ProblemInput*
⟨5⟩ QED
BY ⟨5⟩1, *FS_Subset*
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2, *FS_Subset*
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2
⟨2⟩ QED
BY ⟨2⟩1, *FS_CardinalityType* DEF *Card*

⟨1⟩20. SUFFICES
ASSUME $\neg IsAMinCover(H,\ Xinit,\ Yinit,\ Leq)$
PROVE FALSE
⟨2⟩1. $IsAMinCover(H,\ Xinit,\ Yinit,\ Leq)$
BY ⟨1⟩20
⟨2⟩2. $IsAMinCover(H3,\ Xinit,\ Yinit,\ Leq)$
BY ⟨1⟩17
⟨2⟩3. $Card(H) = Card(H3)$
⟨3⟩3. $\lor\ Card(H) \leq Card(H3)$
$\lor\ Card(H) \geq Card(H3)$
BY ⟨1⟩19
⟨3⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨3⟩3, *HaveCardAsCost*, *ProblemInput*, *FS_Subset*, *AllMinCoversSameCard* DEF *Card*
⟨2⟩4. $Card(H) = Card(C) + Card(E)$
BY ⟨1⟩18, ⟨2⟩3
⟨2⟩5. $Card(H) = Card(C) + Card(E')$
BY ⟨2⟩4, ⟨1⟩4
⟨2⟩ QED goal from ⟨1⟩3
BY ⟨2⟩1, ⟨2⟩5
⟨1⟩21. $H \in CoversOf(Xinit,\ Yinit,\ Leq)$
BY ⟨1⟩8 DEF *IsACoverFrom*, *CoversOf*
⟨1⟩22. $Card(H) > Card(H3)$
⟨2⟩1. $Card(H) \geq Card(H3)$
⟨3⟩1. $H \in CoversOf(Xinit,\ Yinit,\ Leq)$
BY ⟨1⟩21
⟨3⟩2. $IsAMinCover(H3,\ Xinit,\ Yinit,\ Leq)$
BY ⟨1⟩17
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, ⟨1⟩19, *HaveCardAsCost*, *MinCoverHasMinCard*, *ProblemInput* DEF *Card*, *CoversOf*
⟨2⟩2. ASSUME $Card(H) = Card(H3)$
PROVE FALSE
⟨3⟩4. $IsAMinCover(H,\ Xinit,\ Yinit,\ Leq)$
BY ⟨1⟩17, *HaveCardAsCost*, ⟨1⟩21, ⟨2⟩2, *MinCoverEquivCoverCard*, *ProblemInput*, *FS_Subset* DEF *CoversOf*, *Card*
⟨3⟩ QED
BY ⟨3⟩4, ⟨1⟩20
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨1⟩19
⟨1⟩23. $IsFiniteSet(C) \land IsFiniteSet(E)$
⟨2⟩1. $(C \subseteq Y') \land (Y' \subseteq Z) \land IsFiniteSet(Z)$

BY $\langle 1\rangle 7$, *ProblemInput*, *MinCoverProperties*
DEF *IsAMinCover*, *TypeInv*
$\langle 2\rangle 2$. *IsFiniteSet*(C)
BY $\langle 2\rangle 1$, *FS_Subset*
$\langle 2\rangle 3$. $(E \in \text{SUBSET } Z) \land \mathit{IsFiniteSet}(Z)$
BY *ProblemInput* DEF *TypeInv*
$\langle 2\rangle 4$. *IsFiniteSet*(E)
BY $\langle 2\rangle 3$, *FS_Subset*
$\langle 2\rangle$ QED
BY $\langle 2\rangle 2$, $\langle 2\rangle 4$
$\langle 1\rangle 24$. $\mathit{Card}(H) > \mathit{Card}(C) + \mathit{Card}(E)$
BY $\langle 1\rangle 18$, $\langle 1\rangle 22$
$\langle 1\rangle 25$. $\mathit{Card}(H) \leq \mathit{Card}(C) + \mathit{Card}(E)$
$\langle 2\rangle 1$. $(C \cap E) = \{\}$
$\langle 3\rangle 1$. $(Y' \cap E') = \{\}$
OBVIOUS
$\langle 3\rangle 2$. $(Y' \cap E) = \{\}$
BY $\langle 3\rangle 1$, $\langle 1\rangle 4$
$\langle 3\rangle 3$. $C \subseteq Y'$
BY $\langle 1\rangle 3$, *MinCoverProperties*
$\langle 3\rangle$ QED
BY $\langle 3\rangle 2$, $\langle 3\rangle 3$
$\langle 2\rangle 2$. $\mathit{Card}(C \cup E) = \mathit{Card}(C) + \mathit{Card}(E)$
$\langle 3\rangle 1$. $\mathit{Cardinality}(C \cup E) = \mathit{Cardinality}(C) + \mathit{Cardinality}(E)$
$- \mathit{Cardinality}(C \cap E)$
BY $\langle 1\rangle 23$, *FS_Union*
$\langle 3\rangle 2$. $\land \mathit{Cardinality}(C) \in \mathit{Nat}$
$\land \mathit{Cardinality}(E) \in \mathit{Nat}$
$\land \mathit{Cardinality}(C \cap E) = 0$
BY $\langle 1\rangle 23$, *FS_CardinalityType*, $\langle 2\rangle 1$, *FS_EmptySet*
$\langle 3\rangle$ QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$ DEF *Card*
$\langle 2\rangle 3$. $\mathit{Card}(H) \leq \mathit{Card}(C \cup E)$
BY $\langle 1\rangle 7$ DEF *IsAHat*, *Card*
$\langle 2\rangle$ QED
BY $\langle 2\rangle 2$, $\langle 2\rangle 3$
$\langle 1\rangle$ QED goal from $\langle 1\rangle 20$
BY $\langle 1\rangle 24$, $\langle 1\rangle 25$, $\langle 1\rangle 19$, $\langle 1\rangle 23$, *FS_CardinalityType* DEF *Card*

Row reduction leaves the set of (minimal) covers unchanged.
THEOREM *HatIsMinCoverUnchangedByReduceRows* $\triangleq$
ASSUME
$\land$ *HatIsMinCover* $\land$ *TypeInv*
$\land$ *ReduceRows*

PROVE
$HatIsMinCover'$
PROOF
⟨1⟩1. SUFFICES
ASSUME NEW C, NEW H,
$\land \quad IsAMinCover(C,\ X',\ Y',\ Leq)$
$\land \quad IsAHat(H,\ C \cup E',\ Yinit,\ Leq)$
PROVE
$\land\ IsAMinCover(H,\ Xinit,\ Yinit,\ Leq)$
$\land\ Card(H) = Card(C) + Card(E')$
BY DEF $HatIsMinCover$, $Card$
⟨1⟩2. $\land\ E' = E$
$\land\ X' = RowRed(X,\ Y)$
$\land\ Y' = Y$
BY DEF $ReduceRows$
⟨1⟩3. $IsAMinCover(C,\ X,\ Y,\ Leq)$
⟨2⟩1. $IsAMinCover(C,\ X',\ Y,\ Leq)$
BY ⟨1⟩1, ⟨1⟩2
⟨2⟩2. $X' = MaxCeilings(X,\ Y,\ Leq)$
BY ⟨1⟩2 DEF $RowRed$
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, $ProblemInput$, $MinCoverProperties$,
$MinCoverUnchangedByMaxCeil$ DEF Z, $TypeInv$
⟨1⟩4. $IsAHat(H,\ C \cup E,\ Yinit,\ Leq)$
⟨2⟩1. $IsAHat(H,\ C \cup E',\ Yinit,\ Leq)$
BY ⟨1⟩1
⟨2⟩2. $E' = E$
BY ⟨1⟩2
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2
⟨1⟩5. $\land\ IsAMinCover(C,\ X,\ Y,\ Leq)$
$\land\ IsAHat(H,\ C \cup E,\ Yinit,\ Leq)$
BY ⟨1⟩3, ⟨1⟩4
⟨1⟩6. $\land\ IsAMinCover(H,\ Xinit,\ Yinit,\ Leq)$
$\land\ Card(H) = Card(C) + Card(E)$
BY ⟨1⟩5 DEF $HatIsMinCover$, $Card$
⟨1⟩7. $Card(H) = Card(C) + Card(E')$
⟨2⟩1. $Card(H) = Card(C) + Card(E)$
BY ⟨1⟩6
⟨2⟩2. $E' = E$
BY ⟨1⟩2
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2
⟨1⟩8. QED goal from ⟨1⟩1
BY ⟨1⟩6, ⟨1⟩7

If C is a cover after, then $C \cup E'$ is a cover before.

THEOREM $HatIsMinCoverUnchangedByRemoveEssential \triangleq$

ASSUME

$\land\ TypeInv \land TypeInv'$

$\land\ (Y \cap E) = \{\}$

$\land\ (i = 3) \Rightarrow \land\ X = RowRed(Xold,\ Y)$

$\land\ Y = ColRed(Xold,\ Yold)$

$\land\ HatIsMinCover$

$\land\ RemoveEssential$

PROVE

$HatIsMinCover'$

PROOF

$\langle 1 \rangle 14.\ \land\ X = Maxima(X,\ Leq)$

$\land\ Y = Maxima(Y,\ Leq)$

$\langle 2 \rangle 1.\ \land\ X = RowRed(Xold,\ Y)$

$\land\ Y = ColRed(Xold,\ Yold)$

BY DEF $RemoveEssential$

$\langle 2 \rangle$ QED

BY $\langle 2 \rangle 1$, $MaxIsIdempotent$ DEF $RowRed$, $MaxCeilings$, $ColRed$, $MaxFloors$

$\langle 1 \rangle$ USE DEF $Card$

$\langle 1 \rangle 1.$ SUFFICES

ASSUME NEW Ce, NEW H,

$\land\ \ IsAMinCover(Ce,\ X',\ Y',\ Leq)$

$\land\ \ IsAHat(H,\ Ce \cup E',\ Yinit,\ Leq)$

PROVE

$\land\ IsAMinCover(H,\ Xinit,\ Yinit,\ Leq)$

$\land\ Card(H) = Card(Ce) + Card(E')$

BY DEF $HatIsMinCover$

applied for $HatIsMinCover'$

$\langle 1 \rangle$ DEFINE

$Ess \triangleq X \cap Y$

$C \triangleq Ce \cup Ess$

$\langle 1 \rangle 2.\ \land\ X' = X \setminus Ess$

$\land\ Y' = Y \setminus Ess$

BY DEF $RemoveEssential$

$\langle 1 \rangle 3.\ (Ce \cap Ess) = \{\}$

$\langle 2 \rangle 1.\ Ce \subseteq Y'$

BY $\langle 1 \rangle 1$, $MinCoverProperties$

$\langle 2 \rangle 2.\ (Y' \cap Ess) = \{\}$

$\langle 3 \rangle 1.\ Y' = Y \setminus Ess$

BY $\langle 1 \rangle 2$

$\langle 3 \rangle$ QED

BY $\langle 3 \rangle 1$

$\langle 2 \rangle$ QED

BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$

⟨1⟩4. $IsAMinCover(C,\ X,\ Y,\ Leq)$
  ⟨2⟩1. $X = Maxima(X,\ Leq)$
    BY ⟨1⟩14
  ⟨2⟩2. $Y = Maxima(Y,\ Leq)$
    BY ⟨1⟩14
  ⟨2⟩ DEFINE
    $Xe \triangleq X'$
    $Ye \triangleq Y'$
  ⟨2⟩4. $\land\ IsAMinCover(Ce,\ Xe,\ Ye,\ Leq)$
    $\land\ Ess = X \cap Y$
    $\land\ Xe = X \setminus Ess$
    $\land\ Ye = Y \setminus Ess$
    BY ⟨1⟩1, ⟨1⟩2 DEF $Xe,\ Ye,\ Ess$

  ⟨2⟩5. $\land\ C = Ce \cup Ess$
    $\land\ Ce\ = C \setminus Ess$

    ⟨3⟩1. $C = Ce \cup Ess$
      BY DEF C
    ⟨3⟩2. $Ce = C \setminus Ess$
      ⟨4⟩1. SUFFICES $(Ce \cap Ess) = \{\}$
        BY DEF C
      ⟨4⟩ QED goal from ⟨4⟩1
        BY ⟨1⟩3
    ⟨3⟩ QED
      BY ⟨3⟩1, ⟨3⟩2
  ⟨2⟩ HIDE DEF C
  ⟨2⟩ QED
    BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩4, ⟨2⟩5, $HaveCardAsCost$, $ProblemInput$, $MinCoverUnchangedByEssential$ DEF $TypeInv$, Z
⟨1⟩5. ASSUME
    $\land\ IsAMinCover(C,\ X,\ Y,\ Leq)$
    $\land\ IsAHat(H,\ C \cup E,\ Yinit,\ Leq)$
  PROVE
    $\land\ IsAMinCover(H,\ Xinit,\ Yinit,\ Leq)$
    $\land\ Card(H) = Card(C) + Card(E)$
  BY ⟨1⟩5 DEF $HatIsMinCover$
    applied for $HatIsMinCover$
⟨1⟩6. $(Ce \cup E') = (C \cup E)$
  ⟨2⟩1. $(Ce \cup E') = (Ce \cup (E \cup Ess))$
    ⟨3⟩1. $E' = E \cup Ess$
      BY DEF $RemoveEssential$, Ess
    ⟨3⟩ QED
      BY ⟨3⟩1
  ⟨2⟩2. $(Ce \cup (E \cup Ess)) = ((Ce \cup Ess) \cup E)$

OBVIOUS

⟨2⟩3. $((Ce \cup Ess) \cup E) = (C \cup E)$
BY DEF C

⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3

⟨1⟩7. $IsAHat(H,\ C \cup E,\ Yinit,\ Leq)$

⟨2⟩1. $IsAHat(H,\ Ce \cup E',\ Yinit,\ Leq)$
BY ⟨1⟩1

⟨2⟩2. $(Ce \cup E') = (C \cup E)$
BY ⟨1⟩6

⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2

⟨1⟩8. $\land\ IsAMinCover(C,\ X,\ Y,\ Leq)$
$\land\ IsAHat(H,\ C \cup E,\ Yinit,\ Leq)$
BY ⟨1⟩4, ⟨1⟩7

⟨1⟩9. $\land\ IsAMinCover(H,\ Xinit,\ Yinit,\ Leq)$
$\land\ Card(H) = Card(C) + Card(E)$
BY ⟨1⟩8, ⟨1⟩5

⟨1⟩10. $\land\ IsFiniteSet(H) \land IsFiniteSet(Ce)$
$\land\ IsFiniteSet(E) \land IsFiniteSet(Ess)$

⟨2⟩1. $H \subseteq Yinit$
BY ⟨1⟩1 DEF $IsAHat$

⟨2⟩2. $Ess \subseteq Y$
BY DEF Ess

⟨2⟩3. $Ce \subseteq Y'$
BY ⟨1⟩1, $MinCoverProperties$

⟨2⟩4. $Y \in \text{SUBSET } Z \land E \in \text{SUBSET } Z$
BY DEF $TypeInv$

⟨2⟩5. $Y' \in \text{SUBSET } Z$
BY DEF $TypeInv$

⟨2⟩6. $Yinit \subseteq Z$
BY $ProblemInput$

⟨2⟩7. $IsFiniteSet(Z)$
BY $ProblemInput$

⟨2⟩8. $\land\ IsFiniteSet(Y) \land IsFiniteSet(Yinit)$
$\land\ IsFiniteSet(Y') \land IsFiniteSet(E)$
BY ⟨2⟩4, ⟨2⟩5, ⟨2⟩6, ⟨2⟩7, FS_Subset

⟨2⟩9. $\land\ IsFiniteSet(Ce) \land IsFiniteSet(Ess) \land IsFiniteSet(H)$
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩8, FS_Subset

⟨2⟩ QED
BY ⟨2⟩8, ⟨2⟩9

⟨1⟩11. $Card(C) = Card(Ce) + Card(Ess)$

⟨2⟩1. $C = Ce \cup Ess$
BY DEF C

⟨2⟩2. $(Ce \cap Ess) = \{\}$

BY ⟨1⟩3
⟨2⟩3. $IsFiniteSet(Ce)$
BY ⟨1⟩10
⟨2⟩4. $IsFiniteSet(Ess)$
BY ⟨1⟩10
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, *FS_UnionDisjoint*
⟨1⟩12. $Card(H) = (Card(Ce) + Card(Ess)) + Card(E)$
⟨2⟩1. $Card(H) = Card(C) + Card(E)$
BY ⟨1⟩9
⟨2⟩2. $Card(C) = Card(Ce) + Card(Ess)$
BY ⟨1⟩11
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2
⟨1⟩13. $\wedge\, (Card(H) \in Nat) \wedge (Card(Ce) \in Nat)$
$\wedge\, (Card(E) \in Nat) \wedge (Card(Ess) \in Nat)$
BY ⟨1⟩10, *FS_CardinalityType*
⟨1⟩15. $Card(H) = Card(Ce) + Card(E')$
⟨2⟩1. $Card(H) = Card(Ce) + (Card(Ess) + Card(E))$
BY ⟨1⟩12, ⟨1⟩13
⟨2⟩2. $Card(E') = Card(Ess) + Card(E)$
⟨3⟩1. $E' = (Ess \cup E)$
BY DEF *RemoveEssential*, *Ess*
⟨3⟩2. $(Ess \cap E) = \{\}$
⟨4⟩1. $Ess = (X \cap Y)$
BY DEF *Ess*
⟨4⟩2. $Ess \subseteq Y$
BY ⟨4⟩1
⟨4⟩3. $(Y \cap E) = \{\}$
OBVIOUS
⟨4⟩ QED
BY ⟨4⟩2, ⟨4⟩3
⟨3⟩3. $IsFiniteSet(E) \wedge IsFiniteSet(Ess)$
BY ⟨1⟩10
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, *FS_UnionDisjoint*
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2
⟨1⟩ QED goal from ⟨1⟩1
BY ⟨1⟩9, ⟨1⟩15

Any minimal covers of X, Y yield (via *Hat*) a minimal cover of the initial problem *Xinit*, *Yinit*.

THEOREM $RecoveringMinCover \triangleq$
$Spec \Rightarrow \Box HatIsMinCover$
PROOF
⟨1⟩ DEFINE
$InvYE \triangleq (Y \cap E) = \{\}$
$InvMaxAtEss \triangleq (i = 3) \Rightarrow \land X = RowRed(Xold,\ Y)$
$\land Y = ColRed(Xold,\ Yold)$
$Nx \triangleq$
$\land\ Next$
$\land\ TypeInv \land TypeInv'$
$\land\ InvYE \land InvYE'$
$\land\ InvMaxAtEss$
$\land\ Refines(Xinit,\ X \cup E,\ Leq)$
$\land\ Refines(Y \cup E,\ Yinit,\ Leq)$
⟨1⟩ HIDE DEF $InvYE,\ InvMaxAtEss,\ Nx$
⟨1⟩1. ASSUME
$\land\ Nx$
$\land\ HatIsMinCover$
PROVE
$HatIsMinCover'$
BY ⟨1⟩1, $HatIsMinCoverUnchangedByReduceColumns$,
$HatIsMinCoverUnchangedByReduceRows$,
$HatIsMinCoverUnchangedByRemoveEssential$
DEF $Next,\ InvYE,\ InvMaxAtEss,\ Nx$
⟨1⟩2. ASSUME $\land\ HatIsMinCover$
$\land\ [Nx]_{vars}$
PROVE $HatIsMinCover'$
BY ⟨1⟩1, ⟨1⟩2 DEF $HatIsMinCover,\ vars$
⟨1⟩3. $(HatIsMinCover \land \Box[Nx]_{vars}) \Rightarrow \Box HatIsMinCover$
BY ⟨1⟩2, PTL
⟨1⟩4. $(Init \land \Box[Nx]_{vars}) \Rightarrow \Box HatIsMinCover$
BY ⟨1⟩3, $HatIsMinCoverInit$
⟨1⟩5. $\lor \neg \land Spec$
$\land \Box TypeInv$
$\land \Box InvYE$
$\land \Box InvMaxAtEss$
$\land \Box Refines(Xinit,\ X \cup E,\ Leq)$
$\land \Box Refines(Y \cup E,\ Yinit,\ Leq)$
$\lor \Box HatIsMinCover$
BY ⟨1⟩4, PTL DEF $Nx,\ Spec$
⟨1⟩6. $Spec \Rightarrow \Box InvMaxAtEss$
⟨2⟩1. $\lor \neg \lor i \neq 3$
$\lor \land X = RowRed(Xold,\ Y)$
$\land Y = ColRed(Xold,\ Yold)$
$\lor InvMaxAtEss$

BY DEF *InvMaxAtEss*

⟨2⟩ QED
BY ⟨2⟩1, *MaximalAtEss*, *PTL*

⟨1⟩ QED
BY ⟨1⟩5, *TypeOK*, *noYcapE*, ⟨1⟩6, *XinitRefinesXE*, *YERefinesYinit*, *PTL* DEF *InvYE*

Proof that covering X with elements from Y remains feasible.

THEOREM $RemainsFeasible \triangleq Spec \Rightarrow \Box IsFeasible$

PROOF

⟨1⟩ DEFINE
$InvMaxAtEss \triangleq (i = 3) \Rightarrow \land X = RowRed(Xold, Y)$
$\land Y = ColRed(Xold, Yold)$

⟨1⟩1. ASSUME $InitIsFeasible \land Init \land TypeInv$
PROVE $IsFeasible$

⟨2⟩ DEFINE
$Covers \triangleq CoversOf(X, Y, Leq)$
$PZ \triangleq$ SUBSET Z

⟨2⟩ HIDE DEF *Covers*, *PZ*

⟨2⟩1. SUFFICES $\exists Q \in Covers : IsMinimal(Q, Covers, CostLeq)$
BY ⟨2⟩1 DEF *IsFeasible*, *IsAMinCover*, *Covers*

⟨2⟩2. $Covers \neq \{\}$

⟨3⟩1. PICK $C : IsACoverFrom(C, Xinit, Yinit, Leq)$
BY ⟨1⟩1 DEF *InitIsFeasible*

⟨3⟩2. $(X = Xinit) \land (Y = Yinit)$
BY ⟨1⟩1 DEF *Init*

⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, *MinCoverProperties* DEF *Covers*, *CoversOf*, *IsACoverFrom*

⟨2⟩3. $\land Covers \subseteq$ SUBSET Z
$\land IsFiniteSet(Covers)$
$\land IsFiniteSet(Z)$

⟨3⟩1. $Covers \subseteq$ SUBSET Y
BY DEF *Covers*, *CoversOf*

⟨3⟩2. $\land Y \subseteq Z$
$\land IsFiniteSet(Z)$
BY ⟨1⟩1, *ProblemInput*, *FS_Subset* DEF *TypeInv*

⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, *FS_SUBSET*, *FS_Subset*

⟨2⟩ DEFINE
$S \triangleq \{Cardinality(u) : u \in Covers\}$
$leq \triangleq [c \in S \times S \mapsto c[1] \leq c[2]]$
⟨2⟩ HIDE DEF S, leq
⟨2⟩7. $\wedge S \in$ SUBSET Nat
$\wedge S \neq \{\}$
$\wedge IsFiniteSet(S)$
$\wedge S = Support(leq)$
⟨4⟩1. $S \in$ SUBSET Nat
⟨5⟩1. SUFFICES ASSUME NEW $u \in Covers$
PROVE $Cardinality(u) \in Nat$
BY ⟨5⟩1 DEF S
⟨5⟩2. $u \in$ SUBSET Z
BY ⟨5⟩1, ⟨2⟩3
⟨5⟩ QED goal from ⟨5⟩1
BY ⟨2⟩3, *FS_Subset*, *FS_CardinalityType*
⟨4⟩2. $S = Support(leq)$
BY *SupportOfSymmetricDomain* DEF leq
⟨4⟩3. $S \neq \{\}$
BY ⟨2⟩2 DEF S
⟨4⟩4. $IsFiniteSet(S)$
BY *ImageOfFinite*, ⟨2⟩3 DEF S
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3, ⟨4⟩4
⟨2⟩4. PICK $v \in S : IsMinimal(v, S, leq)$
⟨3⟩2. $IsTransitive(leq)$
⟨4⟩1. SUFFICES
ASSUME
NEW $x \in S$, NEW $y \in S$, NEW $z \in S$,
$leq[\langle x, y\rangle] \wedge leq[\langle y, z\rangle]$
PROVE
$leq[\langle x, z\rangle]$
BY ⟨4⟩1, ⟨2⟩7 DEF *IsTransitive*
⟨4⟩2. $x \leq y \ \wedge \ y \leq z$
BY ⟨4⟩1 DEF leq
⟨4⟩3. $x \in Nat \ \wedge \ y \in Nat \ \wedge \ z \in Nat$
BY ⟨4⟩1, ⟨2⟩7
⟨4⟩4. $x \leq z$
BY ⟨4⟩2, ⟨4⟩3
⟨4⟩ QED goal from ⟨4⟩1
BY ⟨4⟩1, ⟨4⟩4 DEF leq
⟨3⟩3. $IsAntiSymmetric(leq)$
⟨4⟩1. SUFFICES
ASSUME
NEW $x \in S$, NEW $y \in S$,

$leq[x,\ y]\ \land\ x \neq y$
PROVE
$\neg leq[y,\ x]$
BY $\langle 4\rangle 1$, $\langle 2\rangle 7$ DEF *IsAntiSymmetric*
$\langle 4\rangle 2.\ x \leq y$
BY $\langle 4\rangle 1$ DEF *leq*
$\langle 4\rangle 3.\ x < y$
BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 2\rangle 7$
$\langle 4\rangle 4.\ \neg(y \leq x)$
$\langle 5\rangle 1.\ x \in Nat\ \land\ y \in Nat$
BY $\langle 4\rangle 1$, $\langle 2\rangle 7$
$\langle 5\rangle$ QED
BY $\langle 4\rangle 3$, $\langle 5\rangle 1$
$\langle 4\rangle$ QED
BY $\langle 4\rangle 4$, $\langle 4\rangle 1$ DEF *leq*
$\langle 3\rangle$ QED
BY $\langle 2\rangle 7$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, *FiniteSetHasMinimal*

$\langle 2\rangle 5$. PICK $Q \in Covers :\ v = Cardinality(Q)$
BY $\langle 2\rangle 4$ DEF S
$\langle 2\rangle 6$. ASSUME NEW $W \in Covers$, $CostLeq[\langle W,\ Q\rangle]$
PROVE $CostLeq[\langle Q,\ W\rangle]$
$\langle 3\rangle$ DEFINE $u \triangleq Cardinality(W)$
$\langle 3\rangle$ HIDE DEF u
$\langle 3\rangle 1.\ u \in S$
BY $\langle 2\rangle 6$ DEF u, S
$\langle 3\rangle 2.\ leq[u,\ v] \Rightarrow leq[v,\ u]$
BY $\langle 2\rangle 4$, $\langle 3\rangle 1$ DEF *IsMinimal*
$\langle 3\rangle 3.\ v \leq u$
$\langle 4\rangle 1.\ u \in Nat\ \land\ v \in Nat$
BY $\langle 2\rangle 4$, $\langle 3\rangle 1$, $\langle 2\rangle 7$
$\langle 4\rangle 2.\ (u \leq v)\ \Rightarrow\ (v \leq u)$
BY $\langle 3\rangle 2$, $\langle 2\rangle 4$, $\langle 3\rangle 1$ DEF *leq*
$\langle 4\rangle$ QED
BY $\langle 4\rangle 1$, $\langle 4\rangle 2$
$\langle 3\rangle 4.\ Cardinality(Q) \leq Cardinality(W)$
BY $\langle 3\rangle 3$, $\langle 2\rangle 5$ DEF u
$\langle 3\rangle$ QED
BY $\langle 2\rangle 5$, $\langle 2\rangle 6$, $\langle 3\rangle 4$, *HaveCardAsCost*, $\langle 2\rangle 3$, *CostLeqToCard* DEF Z
$\langle 2\rangle$ QED goal from $\langle 2\rangle 1$
BY $\langle 2\rangle 5$, $\langle 2\rangle 6$ DEF *IsMinimal*

$\langle 1\rangle 2$. ASSUME
$\land\ IsFeasible$

$\land$ *TypeInv* $\land$ *TypeInv*$'$
$\land$ *InvMaxAtEss*
$\land$ *Next*
PROVE *IsFeasible*$'$

$\langle 2\rangle 1$. ASSUME
IsFeasible $\land$ *TypeInv* $\land$ *ReduceColumns*
PROVE
IsFeasible$'$
$\langle 3\rangle 1$. PICK C : *IsAMinCover*(C, X, Y, *Leq*)
BY $\langle 2\rangle 1$ DEF *IsFeasible*
$\langle 3\rangle$ DEFINE
$Cf \triangleq Floors(C, X, Leq)$
$Yf \triangleq Floors(Y, X, Leq)$
$Cm \triangleq MaxHat(Cf, Yf, Leq)$
$Ymf \triangleq Maxima(Yf, Leq)$
$\langle 3\rangle$ HIDE DEF Cf, Yf, Cm, Ymf
$\langle 3\rangle 2$. $\land$ *IsACompleteLattice*(*Leq*)
$\land$ *IsAPartialOrder*(*Leq*)
$\land$ *CardinalityAsCost*(Z)
$\land$ $X \subseteq Z$
$\land$ $Y \subseteq Z$
$\land$ $Yf \subseteq Z$
$\land$ *IsFiniteSet*(Y)
$\land$ *IsFiniteSet*(Z)
BY $\langle 2\rangle 1$, *ProblemInput*, *HaveCardAsCost*,
FS_Subset, *FloorsIsSubset*
DEF *IsACompleteLattice*, *TypeInv*, Z, Yf
$\langle 3\rangle 3$. *IsAMinCover*(Cf, X, Yf, *Leq*)
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, *MinCoverProperties*,
FloorPreservesMinCover DEF Cf, Yf, Z
$\langle 3\rangle 4$. *IsAMinCover*(Cm, X, Ymf, *Leq*)
BY $\langle 3\rangle 2$, $\langle 3\rangle 3$, *MaxHatOfMinCoverIsAMinCover* DEF Cm, Ymf, Z
$\langle 3\rangle 5$. $\land$ $X' = X$
$\land$ $Y' = Ymf$
BY $\langle 2\rangle 1$ DEF *ReduceColumns*, *ColRed*, Ymf, Yf, *MaxFloors*
$\langle 3\rangle$ QED
BY $\langle 3\rangle 4$, $\langle 3\rangle 5$ DEF *IsFeasible*

$\langle 2\rangle 2$. ASSUME
IsFeasible $\land$ *TypeInv* $\land$ *ReduceRows*
PROVE
IsFeasible$'$
BY $\langle 2\rangle 2$, *MinCoverUnchangedByMaxCeil*,
ProblemInput, *MinCoverProperties*

DEF $ReduceRows$, $RowRed$, Z, $TypeInv$, $IsFeasible$

⟨2⟩3. ASSUME
$\land\ IsFeasible \land RemoveEssential$
$\land\ TypeInv \land TypeInv'$
$\land\ InvMaxAtEss$
PROVE
$IsFeasible'$

⟨3⟩1. $\land\ X = Maxima(X,\ Leq)$
$\land\ Y = Maxima(Y,\ Leq)$
BY ⟨2⟩3, $MaxIsIdempotent$
DEF $InvMaxAtEss$, $RemoveEssential$, $RowRed$, $MaxCeilings$, $ColRed$, $MaxFloors$

⟨3⟩2. $\land\ IsFiniteSet(Z)$
$\land\ CardinalityAsCost(Z)$
$\land\ IsACompleteLattice(Leq)$
BY $ProblemInput$, $HaveCardAsCost$

⟨3⟩3. $\land\ X \subseteq Z$
$\land\ Y \subseteq Z$
BY ⟨2⟩3 DEF $TypeInv$

⟨3⟩4. PICK $C :\ IsAMinCover(C,\ X,\ Y,\ Leq)$
BY ⟨2⟩3 DEF $IsFeasible$

⟨3⟩ DEFINE
$Ess \triangleq X \cap Y$
$Ce \triangleq C \setminus Ess$

⟨3⟩6. $\land\ X' = X \setminus Ess$
$\land\ Y' = Y \setminus Ess$
BY ⟨2⟩3 DEF $RemoveEssential$

⟨3⟩5. $IsAMinCover(Ce,\ X',\ Y',\ Leq)$
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩6, $RemainsMinCoverAfterRemovingEssential$
DEF Ce, Ess, Z

⟨3⟩ QED
BY ⟨3⟩5 DEF $IsFeasible$

⟨2⟩ QED
BY ⟨1⟩2, ⟨2⟩1, ⟨2⟩2, ⟨2⟩3 DEF $Next$

⟨1⟩3. ASSUME $\land\ IsFeasible$
$\land\ [TypeInv \land TypeInv' \land InvMaxAtEss \land Next]_{vars}$
PROVE $IsFeasible'$
BY ⟨1⟩2, ⟨1⟩3 DEF $IsFeasible$, $vars$

⟨1⟩ QED

⟨2⟩1. $\lor \neg \land\ IsFeasible$
$\land \Box[TypeInv \land TypeInv' \land InvMaxAtEss \land Next]_{vars}$
$\lor \Box IsFeasible$
BY ⟨1⟩3, PTL

$\langle 2\rangle 2.\ \vee\ \neg\ \wedge\ Init\ \wedge\ TypeInv$
$\wedge\ \Box[TypeInv\ \wedge\ TypeInv'\ \wedge\ InvMaxAtEss\ \wedge\ Next]_{vars}$
$\vee\ \Box IsFeasible$
BY $\langle 1\rangle 1$, $\langle 2\rangle 1$, $ProblemInput$
$\langle 2\rangle 3.\ \vee\ \neg\ \wedge\ Init$
$\wedge\ \Box\ TypeInv$
$\wedge\ \Box InvMaxAtEss$
$\wedge\ \Box[Next]_{vars}$
$\vee\ \Box IsFeasible$
BY $\langle 2\rangle 2$, PTL
$\langle 2\rangle 4.\ \vee\ \neg\ \wedge\ Spec$
$\wedge\ \Box\ TypeInv$
$\wedge\ \Box InvMaxAtEss$
$\vee\ \Box IsFeasible$
BY $\langle 2\rangle 3$ DEF $Spec$
$\langle 2\rangle 5.\ Spec\ \Rightarrow\ \Box InvMaxAtEss$
$\langle 3\rangle 1.\ \vee\ \neg\ \vee\ i \neq 3$
$\vee\ \wedge\ X = RowRed(Xold,\ Y)$
$\wedge\ Y = ColRed(Xold,\ Yold)$
$\vee\ InvMaxAtEss$
BY DEF $InvMaxAtEss$
$\langle 3\rangle$ QED
BY $\langle 3\rangle 1$, $MaximalAtEss$, PTL
$\langle 2\rangle$ QED
BY $\langle 2\rangle 4$, $\langle 2\rangle 5$, $TypeOK$, PTL

(* Proofs checked with *TLAPS* version 1.4.3 *)

(* The below theorem has been checked by a human. *)

(* Reasoning about termination using the variant. *)

(* Suppose that the cardinalities of both X and Y remained unchanged. It should be $E = \{\}$, otherwise both X and Y would have decreased in cardinality. So X, Y have unchanged cardinality through the row and column reductions. BY *Fixpoint*, the reductions leave both X and Y unchanged. *) THEOREM Termination $\triangleq$
$Spec \Rightarrow ReachesFixpoint$
PROOF
$\langle 1\rangle$ USE DEF $Spec$, $Next$, $ReduceColumns$, $ReduceRows$, $RemoveEssential$, Cardinality
$\langle 1\rangle\ Spec \Rightarrow \Box\Diamond\langle Next\rangle\_i$
$\langle 2\rangle 1.\ Spec \Rightarrow \Box$ENABLED $Next$
OMITTED
$\langle 2\rangle 2.\ Spec \Rightarrow \Box\Diamond\langle Next\rangle\_vars$
BY $\langle 2\rangle 1$
$\langle 2\rangle 3.\ Next \Rightarrow (i' \neq i)$
BY DEF $Next$, $ReduceColumns$, $ReduceRows$, $RemoveEssential$

$\langle 2\rangle 4.\langle Next\rangle\_vars \Rightarrow \langle Next\rangle\_i$
BY $\langle 2\rangle 3$ DEF $vars$
$\langle 2\rangle$ QED
BY $\langle 2\rangle 2, \langle 2\rangle 3$
$\langle 1\rangle 1.\ Spec \Rightarrow \Box(X \subseteq Z \land Y \subseteq Z)$
OMITTED
$\langle 1\rangle 2.\ \land\ Xinit \subseteq Z \land Yinit \subseteq Z$
$\land\ IsFiniteSet(Xinit) \land IsFiniteSet(Yinit)$
OMITTED
$\langle 1\rangle 3.\ Spec \Rightarrow \Diamond\Box[\land\ Cardinality(X) = Cardinality(X')$
$\land\ Cardinality(Y) = Cardinality(Y')]\_vars$
$\langle 2\rangle 1.\ Spec \Rightarrow \Box(IsFiniteSet(X) \land IsFiniteSet(Y))$
$\langle 3\rangle 1.\ IsFiniteSet(Z)$
OBVIOUS
$\langle 3\rangle$ QED
BY $\langle 1\rangle 1, \langle 3\rangle 1$
$\langle 2\rangle 2.\Box[\land\ Cardinality(X') \leq Cardinality(X)$
$\land\ Cardinality(X) \in Nat]\_vars$
BY $\langle 2\rangle 1$, $MaxCeilSmaller$
$(*\ ReduceColumns \Rightarrow (Card(X') = Card(X))*)$
$(*\ ReduceRows \Rightarrow (Card(X') \leq Card(X))*)$
$(*\ RemoveEssential \Rightarrow (Card(X') \leq Card(X))*)$
$\langle 2\rangle 3.\Box[\land\ Cardinality(Y') \leq Cardinality(Y)$
$\land\ Cardinality(Y) \in Nat]\_vars$
BY $\langle 2\rangle 1$, $MaxFloorSmaller$
$(*\ ReduceColumns \Rightarrow (Card(Y') \leq Card(Y))*)$
$(*\ ReduceRows \Rightarrow (Card(Y') = Card(Y))*)$
$(*\ RemoveEssential \Rightarrow (Card(Y') \leq Card(Y))*)$
$\langle 2\rangle$ QED
BY $\langle 2\rangle 2, \langle 2\rangle 3(*\ Well-founded\ induction\ *)$
$\langle 1\rangle 4.\ \lor \neg Spec$
$\lor \Box \lor i \neq 3$
$\lor\ \land X = MaxCeilings(Xold,\ Y,\ Leq)$
$\land\ Y = MaxFloors(Yold,\ Xold,\ Leq)$
OMITTED
$\langle 1\rangle 5.\ \lor \neg Spec$
$\lor \Diamond\Box \lor i \neq 3$
$\lor\ \land X = MaxCeilings(Xold,\ Y,\ Leq)$
$\land\ Y = MaxFloors(Yold,\ Xold,\ Leq)$
BY $\langle 1\rangle 3, \langle 1\rangle 4$
$\langle 1\rangle 6.\ \lor \neg Spec$
$\lor \Diamond\Box \lor i \neq 3$
$\lor\ (X \cap Y) = \{\}$
BY $\langle 1\rangle 3$ DEF $RemoveEssential(*\ otherwise\ X,\ Y\ would\ decrease$
$because\ Ess \triangleq X \cap Y\ would\ be\ non-empty.*)$
$\langle 1\rangle 7.\ \lor \neg Spec$
$\lor \Diamond\Box \lor i \neq 3$
$\lor\ \land X = MaxCeilings(Xold,\ Y,\ Leq)$
$\land\ Y = MaxFloors(Yold,\ Xold,\ Leq)$
$\land\ (X \cap Y) = \{\}$

BY $\langle 1\rangle 5$, $\langle 1\rangle 6$

$\langle 1\rangle 8.\ \lor \neg Spec$
$\lor \Diamond\Box[\lor i \neq 3$
$\lor \land X = MaxCeilings(Xold,\ Y,\ Leq)$
$\land Y = MaxFloors(Yold,\ Xold,\ Leq)$
$\land$ UNCHANGED $\langle X,\ Y\rangle]\_vars$

BY $\langle 1\rangle 7$

$\langle 1\rangle 9.\ \lor \neg Spec$
$\lor \Diamond\Box[\lor i \neq 3$
$\lor \land X = MaxCeilings(X,\ Y,\ Leq)$
$\land Y = MaxFloors(Y,\ X,\ Leq)$
$\land$ UNCHANGED $\langle X,\ Y\rangle]\_vars$

BY $\langle 1\rangle 8$, *Fixpoint*

$\langle 1\rangle 10.\ \lor \neg Spec$
$\lor \Diamond\Box[\lor i \neq 1$
$\lor \land X = MaxCeilings(X,\ Y,\ Leq)$
$\land Y = MaxFloors(Y,\ X,\ Leq)]\_vars$

BY $\langle 1\rangle 9$ DEF *Next*, *RemoveEssential*

$\langle 1\rangle 11.\ \lor \neg Spec$
$\lor \Diamond\Box[\lor i \neq 1$
$\lor \land X = MaxCeilings(X,\ Y,\ Leq)$
$\land Y = MaxFloors(Y,\ X,\ Leq)$
$\land Y' = MaxFloors(Y,\ X,\ Leq)$
$\land$ UNCHANGED $X]\_vars$

BY $\langle 1\rangle 10$ DEF *ReduceColumns*, *ColRed*

$\langle 1\rangle 12.\ \lor \neg Spec$
$\lor \Diamond\Box[\lor i \neq 1$
$\lor \land X = MaxCeilings(X,\ Y,\ Leq)$
$\land Y = MaxFloors(Y,\ X,\ Leq)$
$\land$ UNCHANGED $\langle X,\ Y\rangle]\_vars$

BY $\langle 1\rangle 11$

$\langle 1\rangle 13.\ \lor \neg Spec$
$\lor \Diamond\Box[\lor i \neq 2$
$\lor \land X = MaxCeilings(X,\ Y,\ Leq)$
$\land Y = MaxFloors(Y,\ X,\ Leq)$
$\land X' = MaxCeilings(X,\ Y,\ Leq)$
$\land$ UNCHANGED $Y]\_vars$

BY $\langle 1\rangle 12$ DEF *ReduceRows*, *RowRed*

$\langle 1\rangle 14.\ \lor \neg Spec$
$\lor \Diamond\Box[\lor i \neq 2$
$\lor \land X = MaxCeilings(X,\ Y,\ Leq)$
$\land Y = MaxFloors(Y,\ X,\ Leq)$
$\land$ UNCHANGED $\langle X,\ Y\rangle]\_vars$

BY $\langle 1\rangle 13$

$\langle 1\rangle 15.\ Spec \Rightarrow \Diamond\Box[(i \in 1\ldots 3) \Rightarrow$ UNCHANGED $\langle X,\ Y\rangle]\_vars$

BY $\langle 1\rangle 9$, $\langle 1\rangle 12$, $\langle 1\rangle 14$

$\langle 1\rangle 16.\ Spec \Rightarrow \Box(i \in 1\ldots 3)$

BY *TypeOK*

$\langle 1\rangle$ QED

BY $\langle 1\rangle 15$, $\langle 1\rangle 16$ DEF *vars*, *ReachesFixpoint*

MODULE *StrongReduction*

An algorithm that takes as input the set of minimal covers made of elements from $Maxima(Y, Leq)$ and returns the set of minimal covers from Y. The algorithm is described with Cm as input, which is one minimal cover made of maxima.

The original cyclic core algorithm yields some minimal covers, but not necessarily the entire set of minimal covers. Some minimal covers can be lost with that approach. Instead, the algorithm described below enumerates covers below $Maxima(Y, Leq)$, amending the step where the original algorithm could lose covers.

Author: Ioannis *Filippidis*

EXTENDS
FiniteSetFacts,
FunctionTheorems,
Lattices,
Sequences,
SequenceTheorems,
TLAPS

In order to ensure independence from builtin support of *Sequences* by *TLAPS*, these modules have been developed and checked by replacing the modules *FiniteSets*, *FiniteSetTheorems*, *Sequences*, *SequencesTheorems* with renamed copies, (*FiniteSets_copy* etc.), and appropriately adjusting EXTENDS statements where needed.

CONSTANTS Leq, X, Y

$Z \triangleq Support(Leq)$

ASSUMPTION $CostIsCard \triangleq$
$Cost = [cover \in \text{SUBSET } Z \mapsto Cardinality(cover)]$

ASSUMPTION $ProblemInput \triangleq$
$\land\ IsACompleteLattice(Leq)$
$\land\ IsFiniteSet(Z)$
$\land\ X \subseteq Z$
$\land\ Y \subseteq Z$

THEOREM $XYAreFiniteSets \triangleq$
$\land\ IsFiniteSet(X)$
$\land\ IsFiniteSet(Y)$

PROOF

$\langle 1 \rangle 1.\ \land\ X \subseteq Z$
$\land\ Y \subseteq Z$
BY $ProblemInput$

$\langle 1 \rangle 2.\ IsFiniteSet(Z)$

BY *ProblemInput*
⟨1⟩ QED
BY ⟨1⟩1, ⟨1⟩2, *FS_Subset*

THEOREM $HaveCardAsCost \triangleq CardinalityAsCost(Z)$
PROOF
BY *CostIsCard* DEF *CardinalityAsCost*

THEOREM $LeqIsPor \triangleq IsAPartialOrder(Leq)$
PROOF
BY *ProblemInput* DEF *IsACompleteLattice*

$$Only(ymax,\ C) \triangleq \{u \in X :\ \forall\, yother \in C \setminus \{ymax\} :\ \neg Leq[u,\ yother]\}$$

$$BelowAndSuff(ymax,\ C,\ V) \triangleq \{y \in V :\ \land\, Leq[y,\ ymax]\ \land \forall\, q \in Only(ymax,\ C) :\ Leq[q,\ y]\}$$

Cm is a cover of *X* from $Maxima(Y,\ Leq)$
$$AllCandidatesBelow(Cm,\ V) \triangleq \{S \in \text{SUBSET } V :\ \land\, Cardinality(S) = Cardinality(Cm)$$
unnecessary to consider smaller subsets (they cannot be covers), or larger subsets (they cannot be minimal)
$$\land\, Refines(S,\ Cm,\ Leq)\}$$

If $IsFiniteSet(S)$, then *f* is a bijection, by *FS_NatBijection*.
$$Enumerate(S) \triangleq \text{LET } Dom \triangleq 1\,..\,Cardinality(S) \text{ IN CHOOSE } f :\ f \in Bijection(Dom,\ S)$$

$$Image(f,\ S) \triangleq \{f[x] :\ x \in S\}$$

$$MinCoversOf(U,\ V,\ IsUnder) \triangleq \{C \in \text{SUBSET } V :\ IsAMinCover(C,\ U,\ V,\ IsUnder)\}$$

Specification of the procedure *EnumerateMincoversBelow*.
CONSTANTS *Cm*
VARIABLES *stack*, *MinCoversBelow*

$$Max \triangleq Maxima(Y,\ Leq)$$

$Lm \triangleq Enumerate(Cm)$
$N \triangleq Cardinality(Cm)$ $N = Len(Lm)$
$Patch(r) \triangleq Image(Lm,\ r\ ..\ N)$

$TypeInv \triangleq \land\ stack \in Seq(\text{SUBSET}\ Y)$
$\qquad\qquad\ \land\ MinCoversBelow \subseteq \text{SUBSET}\ Y$

$Init \triangleq \land\ stack = \langle\{\}\rangle$
$\qquad\ \land\ MinCoversBelow = \{\}$

Terminal case that adds a minimal cover to the set *MinCoversBelow*.

$Collect \triangleq$
LET
$end \triangleq Len(stack)$
$Partial \triangleq stack[end]$
$i \triangleq Cardinality(Partial)$
$front \triangleq SubSeq(stack,\ 1,\ end - 1)$
IN
$\land\ i = N$
$\land\ stack' = front$
$\land\ MinCoversBelow' = MinCoversBelow \cup \{Partial\}$

Branching that generates all minimal covers induced by replacing the next maximal element *ymax* with all those below it that suffice (*succ*).

$Expand \triangleq$
LET
$end \triangleq Len(stack)$
$Partial \triangleq stack[end]$
$i \triangleq Cardinality(Partial)$
$k \triangleq i + 1$
$front \triangleq SubSeq(stack,\ 1,\ end - 1)$

$ymax \triangleq Lm[k]$ element to replace
$Q \triangleq Partial \cup Patch(k)$
$succ \triangleq BelowAndSuff(ymax,\ Q,\ Y)$
$enum \triangleq Enumerate(succ)$
$more \triangleq [r \in 1\ ..\ Len(enum) \mapsto Partial \cup \{enum[r]\}]$
IN
$\land\ i < N$
$\land\ stack' = front \circ more$
$\land$ UNCHANGED $MinCoversBelow$

$Next \triangleq$
$\land\ stack \neq \langle\rangle$
$\land\ \lor\ Collect$
$\qquad\ \lor\ Expand$

$vars \triangleq \langle stack,\ MinCoversBelow \rangle$
$Spec \triangleq Init \land \Box[Next]_{vars} \land \mathrm{WF}_{vars}(Next)$

Invariants.

$PartialCoversInStack \triangleq$
$\quad \forall\, si \in \text{DOMAIN } stack :$
$\quad\quad \text{LET}$
$\quad\quad\quad Partial \triangleq stack[si]$
$\quad\quad\quad i \triangleq Cardinality(Partial)$
$\quad\quad\quad k \triangleq i + 1$
$\quad\quad\quad Q \triangleq Partial \cup Patch(k)$
$\quad\quad \text{IN}$
$\quad\quad\quad \land IsAMinCover(Q,\ X,\ Y,\ Leq)$
$\quad\quad\quad \land (Partial \cap Patch(k)) = \{\}$

$LeqToBij(C) \triangleq \text{CHOOSE } g \in Bijection(1\,..\,N,\ C) :$
$\quad \forall\, q \in 1\,..\,N :\ Leq[g[q],\ Lm[q]]$

$IsPrefixCov(PartialCover,\ g) \triangleq$
$\quad \text{LET}$
$\quad\quad i \triangleq Cardinality(PartialCover)$
$\quad \text{IN}$
$\quad\quad PartialCover = \{g[q] :\ q \in 1\,..\,i\}$

$InvCompl(C) \triangleq$
$\quad \text{LET}$
$\quad\quad g \triangleq LeqToBij(C)$
$\quad \text{IN}$
$\quad\quad \lor \exists\, n \in \text{DOMAIN } stack :\ IsPrefixCov(stack[n],\ g)$
$\quad\quad \lor \neg IsAMinCover(C,\ X,\ Y,\ Leq)$
$\quad\quad \lor C \in MinCoversBelow$

$InvSound(C) \triangleq (C \in MinCoversBelow) \Rightarrow IsAMinCover(C,\ X,\ Y,\ Leq)$

Auxiliary theorems about minimal covers.

$\text{THEOREM } SubsetYFinite \triangleq$
$\quad \text{ASSUME NEW } S \in \text{SUBSET } Y$
$\quad \text{PROVE } \land IsFiniteSet(S)$
$\quad\quad\quad\ \land Cardinality(S) \in Nat$
PROOF
BY $XYAreFiniteSets,\ FS\_Subset,\ FS\_CardinalityType$

THEOREM $LmIsBijection \triangleq$
ASSUME
$Cm \in \text{SUBSET } Y$
PROVE
$Lm \in Bijection(1 \,..\, N,\ Cm)$
PROOF
$\langle 1 \rangle 1.\ IsFiniteSet(Cm)$
BY $SubsetYFinite$
$\langle 1 \rangle 2.$ PICK $n \in Nat :\ ExistsBijection(1 \,..\, n,\ Cm)$
BY $\langle 1 \rangle 1,\ FS\_NatBijection$
$\langle 1 \rangle 3.\ n = N$
$\langle 2 \rangle 1.\ Cardinality(Cm) = n$
BY $\langle 1 \rangle 2,\ FS\_CountingElements$
$\langle 2 \rangle 2.\ N = Cardinality(Cm)$
BY DEF N
$\langle 2 \rangle$ QED
BY $\langle 2 \rangle 1,\ \langle 2 \rangle 2$
$\langle 1 \rangle 4.\ ExistsBijection(1 \,..\, N,\ Cm)$
BY $\langle 1 \rangle 2,\ \langle 1 \rangle 3$
$\langle 1 \rangle 5.\ Bijection(1 \,..\, N,\ Cm) \neq \{\}$
BY $\langle 1 \rangle 4$ DEF $ExistsBijection$
$\langle 1 \rangle$ QED
BY $\langle 1 \rangle 5$ DEF $Lm,\ Enumerate,\ N$

THEOREM $NType \triangleq$
ASSUME
$Cm \in \text{SUBSET } Y$
PROVE
$N \in Nat$
PROOF
BY $SubsetYFinite$ DEF N

THEOREM $PatchProperties \triangleq$
ASSUME
NEW $k \in 1 \,..\, (N+1)$,
$Cm \in \text{SUBSET } Y$
PROVE
LET $Pc \triangleq Patch(k)$
IN $\land\ Pc \in \text{SUBSET } Y$
$\land\ Pc \in \text{SUBSET } Cm$
$\land\ IsFiniteSet(Pc)$
$\land\ Cardinality(Pc) = N - k + 1$
PROOF
$\langle 1 \rangle$ DEFINE

$Pc \triangleq Patch(k)$
$R \triangleq k \,..\, N$
⟨1⟩5. $\wedge\, k \in Nat$
$\wedge\, N \in Nat$
BY *NType*
⟨1⟩1. $Pc = \{Lm[x] : x \in R\}$
BY DEF *Pc*, *Patch*, *Image*, *R*
⟨1⟩9. $Lm \in Bijection(1 \,..\, N,\, Cm)$
BY *LmIsBijection*
⟨1⟩2. $\wedge\, R \subseteq$ DOMAIN *Lm*
$\wedge$ DOMAIN $Lm = 1 \,..\, N$
⟨2⟩1. DOMAIN $Lm = 1 \,..\, N$
BY ⟨1⟩9 DEF *Bijection*, *Injection*
⟨2⟩ QED
BY ⟨2⟩1, ⟨1⟩5 DEF *R*
⟨1⟩3. $Lm \in [1 \,..\, N \to Cm]$
BY ⟨1⟩9 DEF *Bijection*, *Injection*
⟨1⟩6. $Pc \subseteq Cm$
BY ⟨1⟩1, ⟨1⟩2, ⟨1⟩3
⟨1⟩4. $IsFiniteSet(Cm)$
⟨2⟩1. $Cm \in$ SUBSET *Y*
OBVIOUS
⟨2⟩ QED
BY ⟨2⟩1, *SubsetYFinite*
⟨1⟩7. $IsFiniteSet(Pc)$
BY ⟨1⟩6, ⟨1⟩4, *FS_Subset*
⟨1⟩8. $Cardinality(Pc) = N - k + 1$
⟨2⟩ DEFINE
$q \triangleq N - k + 1$
$S \triangleq 1 \,..\, q$
$f \triangleq [n \in S \mapsto n - 1 + k]$
$g \triangleq Restrict(Lm,\, R)$
⟨2⟩1. $g \in Bijection(R,\, Pc)$
⟨3⟩1. $Range(g) = Pc$
BY ⟨1⟩1 DEF *g*, *Range*, *Restrict*
⟨3⟩2. $R \in$ SUBSET $1 \,..\, N$
BY ⟨1⟩2
⟨3⟩ QED
BY ⟨1⟩1, ⟨1⟩9, ⟨3⟩1, ⟨3⟩2, *Fun_BijRestrict*
⟨2⟩2. $q \in 0 \,..\, N$
BY ⟨1⟩5
⟨2⟩3. $f \in Bijection(S,\, R)$
⟨3⟩ USE ⟨2⟩2, ⟨1⟩5 DEF *f*
⟨3⟩1. $f \in Injection(S,\, R)$
BY DEF *Injection*

⟨3⟩2. $f \in Surjection(S,\ R)$
BY DEF $Surjection$
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2 DEF $Bijection$
⟨2⟩4. $Cardinality(R) = q$
BY ⟨2⟩3, ⟨2⟩2, $FS\_CountingElements$ DEF $ExistsBijection$
⟨2⟩5. $Cardinality(R) = Cardinality(Pc)$
⟨3⟩1. $IsFiniteSet(R) \land IsFiniteSet(Pc)$
⟨4⟩1. $IsFiniteSet(R)$
BY ⟨2⟩2, ⟨2⟩3, $FS\_NatBijection$ DEF $ExistsBijection$
⟨4⟩2. $IsFiniteSet(Pc)$
BY ⟨1⟩6, $Cm \subseteq Y$, $XYAreFiniteSets$, FS_Subset
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2
⟨3⟩ QED
BY ⟨2⟩1, ⟨3⟩1, $FS\_Bijection$ DEF $ExistsBijection$
⟨2⟩ QED
BY ⟨2⟩4, ⟨2⟩5 DEF q
⟨1⟩ QED
BY ⟨1⟩6, ⟨1⟩7, ⟨1⟩8

THEOREM $PatchSplit \triangleq$
ASSUME
NEW $k \in 1 \,..\, N$,
$\land\ N \in Nat$
$\land\ Cm \in$ SUBSET Y
PROVE
$\land\ Patch(k) = \{Lm[k]\} \cup Patch(k+1)$
$\land\ Lm[k] \notin Patch(k+1)$
PROOF
⟨1⟩ DEFINE
$kp \triangleq k+1$
$S \triangleq k \,..\, N$
$Sp \triangleq kp \,..\, N$
⟨1⟩1. $Patch(k) = Image(Lm,\ S)$
BY DEF $Patch$, S
⟨1⟩2. $Patch(kp) = Image(Lm,\ Sp)$
BY DEF $Patch$, Sp, $Image$
⟨1⟩3. $Image(Lm,\ S) = Image(Lm,\ Sp) \cup \{Lm[k]\}$
⟨2⟩1. $Image(Lm,\ S) = \{Lm[x] :\ x \in S\}$
BY DEF $Image$, S
⟨2⟩2. $Image(Lm,\ Sp) = \{Lm[x] :\ x \in Sp\}$
BY DEF $Image$, Sp
⟨2⟩3. $\{Lm[x] :\ x \in S\} = \{Lm[k]\} \cup \{Lm[x] :\ x \in Sp\}$

```
        ⟨3⟩1. ∧ k  ∈ 1 .. N
              ∧ N ∈ Nat
            OBVIOUS
        ⟨3⟩ QED
            BY ⟨3⟩1  DEF kp, S, Sp
    ⟨2⟩ QED
        BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3
⟨1⟩4. Lm[k] ∉ Patch(k + 1)
    BY LmIsBijection DEF Patch, Bijection, Injection, Image
⟨1⟩ QED
    BY ⟨1⟩1, ⟨1⟩2, ⟨1⟩3, ⟨1⟩4

THEOREM BelowAndSuffIsFinite ≜
    ASSUME
        NEW R, NEW C, NEW ymax,
        IsFiniteSet(R)
    PROVE
        LET S ≜ BelowAndSuff(ymax, C, R)
        IN  IsFiniteSet(S)
PROOF
⟨1⟩ DEFINE
    S ≜ BelowAndSuff(ymax, C, R)
⟨1⟩1. S ⊆ R
    BY  DEF BelowAndSuff
⟨1⟩2. IsFiniteSet(R)
    OBVIOUS
⟨1⟩ QED
    BY ⟨1⟩1, ⟨1⟩2, FS_Subset

THEOREM EnumerateProperties ≜
    ASSUME
        NEW S, IsFiniteSet(S)
    PROVE
        LET
            enum ≜ Enumerate(S)
            Dom ≜ 1 .. Cardinality(S)
        IN
            ∧ enum ∈ Bijection(Dom, S)
            ∧ Len(enum) = Cardinality(S)
            ∧ Len(enum) ∈ Nat
PROOF
⟨1⟩2. PICK n ∈ Nat : ExistsBijection(1 .. n, S)
    ⟨2⟩1. IsFiniteSet(S)
        OBVIOUS
```

⟨2⟩ QED
BY ⟨2⟩1, *FS_NatBijection*
⟨1⟩3. $n = Cardinality(S)$
BY ⟨1⟩2, *FS_CountingElements*
⟨1⟩5. $Bijection(1 \,..\, n,\, S) \neq \{\}$
⟨2⟩1. $ExistsBijection(1 \,..\, n,\, S)$
BY ⟨1⟩2, ⟨1⟩3
⟨2⟩ QED
BY ⟨2⟩1 DEF *ExistsBijection*
⟨1⟩ DEFINE $enum \triangleq Enumerate(S)$
⟨1⟩6. $enum \in Bijection(1 \,..\, n,\, S)$
BY ⟨1⟩5, ⟨1⟩3 DEF *Enumerate*, *enum*
⟨1⟩7. $enum \in Seq(S)$
BY ⟨1⟩2, ⟨1⟩6 DEF *Bijection*, *Injection*, *Seq*
⟨1⟩8. $\wedge$ DOMAIN $enum = 1 \,..\, Len(enum)$
$\wedge\, Len(enum) \in Nat$
BY ⟨1⟩7, *LenProperties*
⟨1⟩9. $enum \in Bijection(1 \,..\, Cardinality(S),\, S)$
BY ⟨1⟩3, ⟨1⟩6
⟨1⟩10. $Len(enum) = Cardinality(S)$
⟨2⟩1. $1 \,..\, Len(enum) = 1 \,..\, Cardinality(S)$
BY ⟨1⟩9, ⟨1⟩8 DEF *Bijection*, *Injection*
⟨2⟩2. $enum \in Bijection(1 \,..\, Len(enum),\, S)$
BY ⟨1⟩9, ⟨2⟩1
⟨2⟩ QED
BY ⟨2⟩2, ⟨1⟩8, *FS_CountingElements* DEF *ExistsBijection*
⟨1⟩ QED
BY ⟨1⟩9, ⟨1⟩8, ⟨1⟩10 DEF *enum*

Auxiliary theorems about minimal covers.

Application of *MinCoversFromMaxSuffice* to current context.
LEMMA *MinCoverFromMaxYIsMinCoverFromY* $\triangleq$
ASSUME
NEW C,
$IsAMinCover(C,\, X,\, Max,\, Leq)$
PROVE
$IsAMinCover(C,\, X,\, Y,\, Leq)$
PROOF
⟨1⟩1. $\wedge\, IsAPartialOrder(Leq)$
$\wedge\, IsFiniteSet(Z)$
$\wedge\, X \subseteq Z$
$\wedge\, Y \subseteq Z$

BY $LeqIsPor$, $ProblemInput$
⟨1⟩2. $CardinalityAsCost(Z)$
BY $HaveCardAsCost$
⟨1⟩ QED
BY ⟨1⟩1, ⟨1⟩2, $MinCoversFromMaxSuffice$ DEF Z, Max

A minimal cover C contains only essential elements. Otherwise, some element $y \in C$ would be redundant, so $(C \setminus \{y\})$ a cover, thus C not minimal.

THEOREM $MinimalHasAllEssential \triangleq$
ASSUME
NEW C,
$IsAMinCover(C, X, Y, Leq)$
PROVE
$\forall\, y \in C : \ Only(y, C) \neq \{\}$
PROOF
⟨1⟩1. SUFFICES
ASSUME
NEW $y \in C$,
$Only(y, C) = \{\}$
PROVE FALSE
OBVIOUS
⟨1⟩ DEFINE $Cy \triangleq C \setminus \{y\}$
⟨1⟩5. $Cy \in$ SUBSET Y
BY $MinCoverProperties$ DEF Cy
⟨1⟩2. $IsACover(Cy, X, Leq)$
⟨2⟩1. SUFFICES ASSUME NEW $x \in X$
PROVE $\exists\, q \in Cy : \ Leq[x, q]$
BY ⟨2⟩1 DEF $IsACover$
⟨2⟩2. SUFFICES ASSUME $\forall\, q \in Cy : \ \neg Leq[x, q]$
PROVE FALSE
BY ⟨2⟩2
⟨2⟩3. $x \in Only(y, C)$
BY ⟨2⟩2 DEF $Only$, Cy
⟨2⟩ QED
BY ⟨2⟩3, ⟨1⟩1
⟨1⟩3. $\wedge\ Cardinality(Cy) < Cardinality(C)$
$\wedge\ Cardinality(Cy) \in Nat$
$\wedge\ Cardinality(C) \in Nat$
⟨2⟩1. $IsFiniteSet(C)$
BY $MinCoverProperties$, $SubsetYFinite$
⟨2⟩2. $Cy \subseteq C$
BY DEF Cy
⟨2⟩3. $Cy \neq C$
⟨3⟩1. $y \in C$

OBVIOUS

⟨3⟩ QED
BY ⟨3⟩1 DEF Cy

⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, FS_Subset, $FS\_CardinalityType$

⟨1⟩4. $Cardinality(C) \leq Cardinality(Cy)$

⟨2⟩1. $\wedge\ Y \in \text{SUBSET}\ Z$
$\wedge\ IsAMinCover(C,\ X,\ Y,\ Leq)$
$\wedge\ CardinalityAsCost(Z)$
BY $ProblemInput$, $HaveCardAsCost$

⟨2⟩2. $\wedge\ Cy \in \text{SUBSET}\ Y$
$\wedge\ IsACover(Cy,\ X,\ Leq)$
$\wedge\ Cardinality(Cy) \leq Cardinality(C)$
BY ⟨1⟩5, ⟨1⟩2, ⟨1⟩3

⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, $MinCoverPropertiesCard$

⟨1⟩ QED
BY ⟨1⟩3, ⟨1⟩4

Any minimal cover C from Y refines some minimal cover Cm from $Maxima(Y,\ Leq)$, and they have the same cardinality. So

$MinCoversOf(X,\ Y,\ Leq) \subseteq \text{UNION}\ \{$
$AllCandidatesBelow(Cm,\ Y) : Cm \in MinCoversOf(X,\ Maxima(Y,\ Leq),\ Leq)\}$

Also, $MinCoversOf(X,\ Maxima(Y),\ Leq)$ induces a partition of $MinCoversOf(X,\ Y,\ Leq)$.

THEOREM $MinCoversSubseteqUnionCandidatesBelow \triangleq$
ASSUME
NEW C,
$IsAMinCover(C,\ X,\ Y,\ Leq)$
PROVE
$\exists\, M :\ \wedge\ IsAMinCover(M,\ X,\ Max,\ Leq)$
$\wedge\ C \in AllCandidatesBelow(M,\ Y)$

PROOF

⟨1⟩ DEFINE
$M \triangleq MaxHat(C,\ Y,\ Leq)$

⟨1⟩1. $IsAMinCover(M,\ X,\ Max,\ Leq)$

⟨2⟩1. $Z = Support(Leq)$
BY DEF Z

⟨2⟩2. $IsAPartialOrder(Leq)$
BY $LeqIsPor$

⟨2⟩3. $\wedge\ IsFiniteSet(Z)$
$\wedge\ X \subseteq Z$
$\wedge\ Y \subseteq Z$
BY $ProblemInput$

⟨2⟩4. $IsAMinCover(C,\ X,\ Y,\ Leq)$

OBVIOUS

⟨2⟩5. $CardinalityAsCost(Z)$

BY $HaveCardAsCost$

⟨2⟩ QED

BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, ⟨2⟩5, $MaxHatOfMinCoverIsAMinCover$ DEF Max, M

⟨1⟩2. $\wedge\ C \in \text{SUBSET}\ Y$
$\wedge\ IsACover(C, X, Leq)$

⟨2⟩1. $IsAMinCover(C, X, Y, Leq)$

OBVIOUS

⟨2⟩2. $C \in CoversOf(X, Y, Leq)$

BY ⟨2⟩1 DEF $IsAMinCover$, $IsMinimal$

⟨2⟩ QED

BY ⟨2⟩2 DEF $CoversOf$

⟨1⟩3. $\wedge\ Refines(C, M, Leq)$
$\wedge\ Cardinality(M) \leq Cardinality(C)$

⟨2⟩1. $Z = Support(Leq)$

BY DEF Z

⟨2⟩2. $IsAPartialOrder(Leq)$

BY $LeqIsPor$

⟨2⟩3. $\wedge\ IsFiniteSet(Z)$
$\wedge\ Y \subseteq Z$

BY $ProblemInput$

⟨2⟩4. $C \subseteq Y$

BY ⟨1⟩2

⟨2⟩ QED

BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, $MaxHatProperties$, $CostIsCard$ DEF M
$S \leftarrow C, H \leftarrow M$

⟨1⟩4. $Cardinality(C) = Cardinality(M)$

⟨2⟩1. $IsAMinCover(C, X, Y, Leq)$

OBVIOUS

⟨2⟩2. $IsAMinCover(M, X, Y, Leq)$

⟨3⟩1. $IsAMinCover(M, X, Max, Leq)$

BY ⟨1⟩1

⟨3⟩ QED

BY ⟨3⟩1, $MinCoversFromMaxSuffice$, $ProblemInput$, $LeqIsPor$, $HaveCardAsCost$ DEF Max, Z

⟨2⟩ QED

BY ⟨2⟩1, ⟨2⟩2, $AllMinCoversSameCard$, $HaveCardAsCost$, $XYAreFiniteSets$, $ProblemInput$
$C \leftarrow C, H \leftarrow M$

⟨1⟩5. $C \in AllCandidatesBelow(M, Y)$

⟨2⟩1. $C \in \text{SUBSET}\ Y$

BY ⟨1⟩2

⟨2⟩2. $Cardinality(C) = Cardinality(M)$

BY ⟨1⟩4
⟨2⟩3. *Refines*(*C*, *M*, *Leq*)
BY ⟨1⟩3
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3 DEF *AllCandidatesBelow*
⟨1⟩ QED
⟨2⟩1. *IsAMinCover*(*M*, *X*, *Max*, *Leq*)
BY ⟨1⟩1
⟨2⟩2. *C* ∈ *AllCandidatesBelow*(*M*, *Y*)
BY ⟨1⟩5
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2 DEF *Max*

Any minimal cover from *Y* is a finite set, because the lattice *Leq* has a finite domain.

THEOREM *MinCoverIsFinite* ≜
ASSUME
NEW *C*,
IsAMinCover(*C*, *X*, *Y*, *Leq*)
PROVE
∧ *IsFiniteSet*(*C*)
∧ *Cardinality*(*C*) ∈ *Nat*
PROOF
⟨1⟩1. *IsFiniteSet*(*C*)
⟨2⟩1. *IsAMinCover*(*C*, *X*, *Y*, *Leq*)
OBVIOUS
⟨2⟩2. *C* ∈ SUBSET *Y*
BY ⟨2⟩1, *MinCoverProperties*
⟨2⟩3. *IsFiniteSet*(*Y*)
BY *XYAreFiniteSets*
⟨2⟩ QED
BY ⟨2⟩2, ⟨2⟩3, *FS_Subset*
⟨1⟩2. *Cardinality*(*C*) ∈ *Nat*
BY ⟨1⟩1, *FS_CardinalityType*
⟨1⟩ QED
BY ⟨1⟩1, ⟨1⟩2

If a minimal cover *C* refines a minimal cover *Cm*, then each *ym* ∈ *Cm* has some *y* ∈ *C* below it.

THEOREM *MinCoverRefinementHasBelow* ≜
ASSUME
NEW *C* ∈ SUBSET *Y*,
NEW *ym* ∈ *Cm*,
∧ *IsAMinCover*(*Cm*, *X*, *Y*, *Leq*)

$\land$ $IsACover(C,\ X,\ Leq)$
$\land$ $Refines(C,\ Cm,\ Leq)$
PROVE
$\exists\, y \in C :\ Leq[y,\ ym]$
PROOF
$\langle 1\rangle 1$. SUFFICES
ASSUME $\forall\, y \in C :\ \neg Leq[y,\ ym]$
PROVE FALSE
BY $\langle 1\rangle 1$
$\langle 1\rangle$ DEFINE
$H \triangleq Cm \setminus \{ym\}$
$\langle 1\rangle 2$. $\land$ $Cm \in$ SUBSET Y
$\land$ $IsFiniteSet(Cm)$
$\land$ $Cardinality(Cm) \in Nat$
$\langle 2\rangle 1$. $IsAMinCover(Cm,\ X,\ Y,\ Leq)$
OBVIOUS
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1$, *MinCoverProperties*, *MinCoverIsFinite*
$\langle 1\rangle 3$. $H \in$ SUBSET Y
$\langle 2\rangle 1$. $H \subseteq Cm$
BY DEF H
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1$, $\langle 1\rangle 2$
$\langle 1\rangle 4$. $IsACover(H,\ X,\ Leq)$
This proof reminds of *MaxHatIsCoverToo*
$\langle 2\rangle 1$. $Refines(C,\ Cm,\ Leq)$
OBVIOUS
$\langle 2\rangle 2$. $\forall\, u \in C :\ \exists\, v \in Cm :\ Leq[u,\ v]$
BY $\langle 2\rangle 1$ DEF *Refines*
$\langle 2\rangle 3$. ASSUME NEW $u \in C$, NEW $v \in Cm$, $Leq[u,\ v]$
PROVE $v \neq ym$
$\langle 3\rangle 1$. SUFFICES ASSUME $v = ym$
PROVE FALSE
BY $\langle 3\rangle 1$
$\langle 3\rangle 2$. $Leq[u,\ ym]$
BY $\langle 2\rangle 3$, $\langle 3\rangle 1$
$\langle 3\rangle 3$. $\neg Leq[u,\ ym]$
BY $\langle 1\rangle 1$, $\langle 2\rangle 3$ $y \leftarrow u$
$\langle 3\rangle$ QED goal from $\langle 3\rangle 1$
BY $\langle 3\rangle 2$, $\langle 3\rangle 3$
$\langle 2\rangle 4$. $\forall\, u \in C :\ \exists\, v \in Cm \setminus \{ym\} :\ Leq[u,\ v]$
BY $\langle 2\rangle 2$, $\langle 2\rangle 3$
$\langle 2\rangle 5$. $IsACover(C,\ X,\ Leq)$
OBVIOUS
$\langle 2\rangle 6$. $\forall\, x \in X :\ \exists\, u \in C :\ Leq[x,\ u]$

BY $\langle 2\rangle 5$ DEF *IsACover*

$\langle 2\rangle 7$. ASSUME NEW $x \in X$
PROVE $\exists\, v \in H :\ Leq[x,\, v]$

$\langle 3\rangle 1$. PICK $u \in C :\ Leq[x,\, u]$
BY $\langle 2\rangle 6$, $\langle 2\rangle 7$

$\langle 3\rangle 2$. PICK $v \in Cm \setminus \{ym\} :\ Leq[u,\, v]$
BY $\langle 2\rangle 4$, $\langle 3\rangle 1$

$\langle 3\rangle 3$. $v \in H$
BY $\langle 3\rangle 2$ DEF H

$\langle 3\rangle 4$. $Leq[x,\, v]$

$\langle 4\rangle 1$. $IsTransitive(Leq)$
BY *LeqIsPor* DEF *IsAPartialOrder*

$\langle 4\rangle 2$. $Z = Support(Leq)$
BY DEF Z

$\langle 4\rangle 3$. $Leq[x,\, u] \land Leq[u,\, v]$
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$

$\langle 4\rangle 4$. $(x \in Z) \land (u \in Z) \land (v \in Z)$

$\langle 5\rangle 1$. $x \in Z$

$\langle 6\rangle 1$. $x \in X$
BY $\langle 2\rangle 7$

$\langle 6\rangle 2$. $X \subseteq Z$
BY *ProblemInput*

$\langle 6\rangle$ QED
BY $\langle 6\rangle 1$, $\langle 6\rangle 2$

$\langle 5\rangle 2$. $u \in Z$

$\langle 6\rangle 1$. $u \in C$
BY $\langle 3\rangle 1$

$\langle 6\rangle 2$. $C \subseteq Z$

$\langle 7\rangle 1$. $C \subseteq Y$
OBVIOUS

$\langle 7\rangle 2$. $Y \subseteq Z$
BY *ProblemInput*

$\langle 7\rangle$ QED
BY $\langle 7\rangle 1$, $\langle 7\rangle 2$

$\langle 6\rangle$ QED
BY $\langle 6\rangle 1$, $\langle 6\rangle 2$

$\langle 5\rangle 3$. $v \in Z$

$\langle 6\rangle 1$. $v \in H$
BY $\langle 3\rangle 3$

$\langle 6\rangle 2$. $H \subseteq Z$

$\langle 7\rangle 1$. $H \subseteq Y$
BY $\langle 1\rangle 3$

$\langle 7\rangle 2$. $Y \subseteq Z$
BY *ProblemInput*

$\langle 7\rangle$ QED

BY $\langle 7\rangle 1$, $\langle 7\rangle 2$

$\langle 6\rangle$ QED

BY $\langle 6\rangle 1$, $\langle 6\rangle 2$

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 4$ DEF *IsTransitive*

$\langle 3\rangle$ QED

BY $\langle 3\rangle 3$, $\langle 3\rangle 4$

$\langle 2\rangle$ QED

BY $\langle 2\rangle 7$ DEF *IsACover*

$\langle 1\rangle 5$. $\land$ *IsFiniteSet*(*Cm*) $\land$ *Cardinality*(*Cm*) $\in$ *Nat*
$\land$ *IsFiniteSet*(*H*) $\land$ *Cardinality*(*H*) $\in$ *Nat*

$\langle 2\rangle 1$. *IsFiniteSet*(*H*) $\land$ *Cardinality*(*H*) $\in$ *Nat*

$\langle 3\rangle 1$. *IsFiniteSet*(*H*)

$\langle 4\rangle 1$. *H* $\in$ SUBSET *Y*

BY $\langle 1\rangle 3$

$\langle 4\rangle 2$. *IsFiniteSet*(*Y*)

BY *XYAreFiniteSets*

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, *FS_Subset*

$\langle 3\rangle 2$. *Cardinality*(*H*) $\in$ *Nat*

BY $\langle 3\rangle 1$, *FS_CardinalityType*

$\langle 3\rangle$ QED

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

$\langle 2\rangle$ QED

BY $\langle 2\rangle 1$, $\langle 1\rangle 2$

$\langle 1\rangle 6$. *Cardinality*(*H*) $<$ *Cardinality*(*Cm*)

BY $\langle 1\rangle 5$, *FS_Subset* DEF *H*

$\langle 1\rangle 7$. *Cardinality*(*Cm*) $\leq$ *Cardinality*(*H*)

$\langle 2\rangle 1$. $\land$ *Cm* $\in$ SUBSET *Y*
$\land$ *IsACover*(*Cm*, *X*, *Leq*)
$\land \forall\, r \in$ SUBSET *Y* :
$\lor \neg \land$ *IsACover*(*r*, *X*, *Leq*)
$\land$ *Cardinality*(*r*) $\leq$ *Cardinality*(*Cm*)
$\lor$ *Cardinality*(*Cm*) $\leq$ *Cardinality*(*r*)

$\langle 3\rangle 1$. *IsAMinCover*(*Cm*, *X*, *Y*, *Leq*)

OBVIOUS

$\langle 3\rangle$ QED

BY $\langle 3\rangle 1$, *HaveCardAsCost*, *ProblemInput*, *MinCoverPropertiesCard*

$\langle 2\rangle 3$. *IsACover*(*H*, *X*, *Leq*)

BY $\langle 1\rangle 4$

$\langle 2\rangle 4$. *Cardinality*(*H*) $\leq$ *Cardinality*(*Cm*)

BY $\langle 1\rangle 6$, $\langle 1\rangle 5$

$\langle 2\rangle$ QED

BY $\langle 2\rangle 1$, $\langle 1\rangle 3$, $\langle 2\rangle 3$, $\langle 2\rangle 4$ $r \leftarrow H$

$\langle 1\rangle$ QED goal from $\langle 1\rangle 1$

BY $\langle 1\rangle 5$, $\langle 1\rangle 6$, $\langle 1\rangle 7$

Analogous to *HasMaxHat*

LEMMA $HasHat \triangleq$

ASSUME

NEW S, NEW T,

$\land S \subseteq Z$

$\land T \subseteq Z$

$\land Refines(S,\ T,\ Leq)$

PROVE

LET

$H \triangleq Hat(S,\ T,\ Leq)$

IN

$IsAHat(H,\ S,\ T,\ Leq)$

$\land H \in \text{SUBSET } T$

$\land Refines(S,\ H,\ Leq)$

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

PROOF

$\langle 1\rangle$ DEFINE

$H \triangleq Hat(S,\ T,\ Leq)$

$\langle 1\rangle 1$. $\land H \in \text{SUBSET } T$

$\land Refines(S,\ H,\ Leq)$

$\langle 2\rangle 1$. $Refines(S,\ T,\ Leq)$

OBVIOUS

$\langle 2\rangle$ QED

BY $\langle 2\rangle 1$ DEF H, Hat, $SomeAbove$, $Refines$

$\langle 1\rangle 2$. $Cardinality(H) \leq Cardinality(S)$

$\langle 2\rangle 1$. $IsFiniteSet(S)$

$\langle 3\rangle 1$. $IsFiniteSet(Z)$

BY $ProblemInput$

$\langle 3\rangle 2$. $S \subseteq Z$

OBVIOUS

$\langle 3\rangle$ QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, FS_Subset

$\langle 2\rangle$ QED

BY $\langle 2\rangle 1$, $ImageOfFinite$ DEF H, Hat

$\langle 1\rangle$ QED

BY $\langle 1\rangle 1$, $\langle 1\rangle 2$

Theorems establishing a bijection using Leq.

If a minimal cover C refines a minimal cover Cm, then no $ym \in Cm$ can cover two elements $a, b \in C$.

THEOREM $AtMostOneBelow \triangleq$
ASSUME
NEW C,
NEW $ym \in Cm$,
NEW $a \in C$, NEW $b \in C$,
$\land IsAMinCover(Cm, X, Y, Leq)$
$\land IsAMinCover(C, X, Y, Leq)$
$\land Refines(C, Cm, Leq)$
$\land a \neq b$
$\land Leq[a, ym]$
$\land Leq[b, ym]$
PROVE
FALSE
PROOF
$\langle 1 \rangle$ DEFINE
$Rest \triangleq C \setminus \{a, b\}$
$H \triangleq Hat(Rest, Cm, Leq)$
$Q \triangleq H \cup \{ym\}$
$k \triangleq Cardinality(C)$
$\langle 1 \rangle 1. \land C \in$ SUBSET Y
$\land Cm \in$ SUBSET Y
$\land IsFiniteSet(C)$
$\land IsFiniteSet(Cm)$
$\land Cardinality(Cm) \in Nat$
$\land Cardinality(C) \in Nat$
$\land k \in Nat$
$\langle 2 \rangle 1. \land C \in$ SUBSET Y
$\land Cm \in$ SUBSET Y
$\langle 3 \rangle 1. \land IsAMinCover(Cm, X, Y, Leq)$
$\land IsAMinCover(C, X, Y, Leq)$
OBVIOUS
$\langle 3 \rangle$ QED
BY $\langle 3 \rangle 1$, *MinCoverProperties*
$\langle 2 \rangle 2.$ $IsFiniteSet(Y)$
BY *XYAreFiniteSets*
$\langle 2 \rangle 3.$ $IsFiniteSet(C) \land IsFiniteSet(Cm)$
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, *FS_Subset*
$\langle 2 \rangle$ QED
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 3$, *FS_CardinalityType*
$\langle 1 \rangle 2. \land H \in$ SUBSET Cm
$\land H \in$ SUBSET Y
$\land IsFiniteSet(H)$
$\land Cardinality(H) \in Nat$

⟨2⟩1. $Refines(Rest,\ Cm,\ Leq)$
⟨3⟩1. $Refines(C,\ Cm,\ Leq)$
OBVIOUS
⟨3⟩2. $Rest \in \text{SUBSET}\ C$
BY DEF $Rest$
⟨3⟩ QED
BY $SubsetRefinesToo$
$S \leftarrow C,\ R \leftarrow Rest,\ T \leftarrow Cm$
⟨2⟩2. $\land\ Rest \in \text{SUBSET}\ Z$
$\land\ Cm \in \text{SUBSET}\ Z$
⟨3⟩1. $Rest \in \text{SUBSET}\ C$
BY DEF $Rest$
⟨3⟩2. $Rest \in \text{SUBSET}\ Y$
BY ⟨3⟩1, ⟨1⟩1
⟨3⟩ QED
BY ⟨1⟩1, ⟨3⟩2, $ProblemInput$
⟨2⟩3. $\land\ H \in \text{SUBSET}\ Cm$
$\land\ Refines(Rest,\ H,\ Leq)$
$\land\ Cardinality(H) \leq Cardinality(Rest)$
BY ⟨2⟩1, ⟨2⟩2, $HasHat$ DEF H
$S \leftarrow Rest,\ T \leftarrow Cm$
⟨2⟩4. $\land\ IsFiniteSet(H)$
$\land\ Cardinality(H) \in Nat$
⟨3⟩1. $H \in \text{SUBSET}\ Cm$
BY ⟨2⟩3
⟨3⟩2. $IsFiniteSet(Cm)$
BY ⟨1⟩1
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, FS_Subset, $FS\_CardinalityType$
⟨2⟩ QED
⟨3⟩1. $(H \subseteq Cm) \land (Cm \subseteq Y)$
BY ⟨2⟩3, ⟨1⟩1
⟨3⟩ QED
BY ⟨3⟩1, ⟨2⟩4
⟨1⟩3. $\land\ Q \in \text{SUBSET}\ Cm$
$\land\ IsFiniteSet(Q)$
$\land\ Cardinality(Q) \in Nat$
$\land\ Cardinality(Q) \leq Cardinality(H) + 1$
⟨2⟩1. $Q \in \text{SUBSET}\ Cm$
⟨3⟩1. $Q = H \cup \{ym\}$
BY DEF Q
⟨3⟩2. $H \subseteq Cm$
BY ⟨1⟩2
⟨3⟩3. $ym \in Cm$
OBVIOUS

⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3
⟨2⟩2. ∧ *IsFiniteSet*(*Q*)
∧ *Cardinality*(*Q*) ≤ *Cardinality*(*H*) + 1
BY ⟨1⟩2, *FS_AddElementUpperBound* DEF *Q*
S ← *H*, *x* ← *ym*
⟨2⟩3. *Cardinality*(*Q*) ∈ *Nat*
BY ⟨2⟩2, *FS_CardinalityType*
⟨2⟩ QED
BY ⟨2⟩2, ⟨2⟩3, ⟨2⟩1
⟨1⟩4. ∧ *IsFiniteSet*(*Rest*)
∧ *Cardinality*(*Rest*) ∈ *Nat*
⟨2⟩1. *Rest* ∈ SUBSET *C*
BY DEF *Rest*
⟨2⟩2. *IsFiniteSet*(*C*)
BY ⟨1⟩1
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, *FS_Subset*, *FS_CardinalityType*
⟨1⟩5. *IsACover*(*Q*, *X*, *Leq*)
⟨2⟩1. *IsACover*(*H*, *Rest*, *Leq*)
⟨3⟩1. ∀ *u* ∈ *C* : ∃ *v* ∈ *Cm* : *Leq*[*u*, *v*]
⟨4⟩1. *Refines*(*C*, *Cm*, *Leq*)
OBVIOUS
⟨4⟩ QED
BY ⟨4⟩1 DEF *Refines*
⟨3⟩2. ∀ *u* ∈ *Rest* : ∃ *v* ∈ *Cm* : *Leq*[*u*, *v*]
BY ⟨3⟩1 DEF *Rest*
⟨3⟩3. ∀ *u* ∈ *Rest* : LET *r* ≜ *SomeAbove*(*u*, *Cm*, *Leq*)
IN *Leq*[*u*, *r*]
BY ⟨3⟩2 DEF *SomeAbove*
⟨3⟩4. ∀ *u* ∈ *Rest* : ∃ *r* ∈ *Hat*(*Rest*, *Cm*, *Leq*) : *Leq*[*u*, *r*]
BY ⟨3⟩3 DEF *Hat*
⟨3⟩5. ∀ *u* ∈ *Rest* : ∃ *r* ∈ *H* : *Leq*[*u*, *r*]
BY ⟨3⟩4 DEF *H*
⟨3⟩ QED
BY ⟨3⟩5 DEF *IsACover*
⟨2⟩2. *IsACover*(*Q*, *C*, *Leq*)
⟨3⟩1. SUFFICES
ASSUME NEW *u* ∈ *C*
PROVE ∃ *v* ∈ *Q* : *Leq*[*u*, *v*]
BY ⟨3⟩1 DEF *IsACover*
⟨3⟩2.CASE *u* ∈ {*a*, *b*}
⟨4⟩1. *Leq*[*u*, *ym*]
⟨5⟩1. ∧ *Leq*[*a*, *ym*]
∧ *Leq*[*b*, *ym*]

OBVIOUS

⟨5⟩ QED

BY ⟨3⟩2, ⟨5⟩1

⟨4⟩2. $ym \in Q$

BY DEF Q

⟨4⟩ QED

BY ⟨4⟩1, ⟨4⟩2

⟨3⟩3. CASE $u \notin \{a, b\}$

⟨4⟩1. $u \in C \setminus \{a, b\}$

BY ⟨3⟩1, ⟨3⟩3

⟨4⟩2. $u \in Rest$

BY ⟨4⟩1 DEF $Rest$

⟨4⟩3. PICK $v \in H : Leq[u, v]$

BY ⟨2⟩1, ⟨4⟩2 DEF $IsACover$

⟨4⟩4. $v \in Q$

BY ⟨4⟩3 DEF Q

⟨4⟩ QED

BY ⟨4⟩3, ⟨4⟩4

⟨3⟩ QED *goal from ⟨3⟩1*

BY ⟨3⟩2, ⟨3⟩3

⟨2⟩3. $IsACover(C, X, Leq)$

⟨3⟩1. $IsAMinCover(C, X, Y, Leq)$

OBVIOUS

⟨3⟩ QED

BY ⟨3⟩1, *MinCoverProperties*

⟨2⟩4. $\wedge\ Q \subseteq Z$
$\wedge\ C \subseteq Z$
$\wedge\ X \subseteq Z$

⟨3⟩1. $Y \subseteq Z$

BY *ProblemInput*

⟨3⟩2. $C \subseteq Z$

⟨4⟩1. $C \subseteq Y$

BY ⟨1⟩1

⟨4⟩ QED

BY ⟨4⟩1, ⟨3⟩1

⟨3⟩3. $Q \subseteq Z$

⟨4⟩1. $Q \subseteq Cm$

BY ⟨1⟩3

⟨4⟩2. $Cm \subseteq Y$

BY ⟨1⟩1

⟨4⟩ QED

BY ⟨4⟩1, ⟨4⟩2, ⟨3⟩1

⟨3⟩4. $X \subseteq Z$

BY *ProblemInput*

⟨3⟩ QED

BY ⟨3⟩2, ⟨3⟩3, ⟨3⟩4

⟨2⟩ QED
BY ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, *ProblemInput*, *LatticeProperties*, *CoveringIsTransitive* DEF Z

⟨1⟩6. $Cardinality(Q) \leq k - 1$

⟨2⟩1. $Cardinality(H) \leq k - 2$

⟨3⟩1. $Cardinality(C \setminus \{a,\ b\}) = k - 2$

⟨4⟩1. $a \in C$

OBVIOUS

⟨4⟩2. $IsFiniteSet(C)$

BY ⟨1⟩1

⟨4⟩3. $\land\ IsFiniteSet(C \setminus \{a\})$
$\land\ Cardinality(C \setminus \{a\}) = Cardinality(C) - 1$

BY ⟨4⟩1, ⟨4⟩2, *FS_RemoveElement*

⟨4⟩4. $Cardinality(C \setminus \{a\}) = k - 1$

BY ⟨4⟩3 DEF k

⟨4⟩5. $b \in (C \setminus \{a\})$

⟨5⟩1. $\land\ a \neq b$
$\land\ b \in C$

OBVIOUS

⟨5⟩ QED
BY ⟨5⟩1

⟨4⟩6. $Cardinality(C \setminus \{a,\ b\}) = Cardinality(C \setminus \{a\}) - 1$

BY ⟨4⟩3, ⟨4⟩5, *FS_RemoveElement*

⟨4⟩ QED
BY ⟨1⟩1, ⟨4⟩4, ⟨4⟩6

⟨3⟩2. $Cardinality(Rest) = k - 2$

BY ⟨3⟩1 DEF *Rest*

⟨3⟩3. $Cardinality(H) \leq Cardinality(Rest)$

BY ⟨1⟩4, *ImageOfFinite* DEF H, *Hat*

⟨3⟩ QED
BY ⟨3⟩2, ⟨3⟩3

⟨2⟩2. $Cardinality(Q) \leq Cardinality(H) + 1$

⟨3⟩1. $\lor\ Cardinality(Q) = Cardinality(H)$
$\lor\ Cardinality(Q) = Cardinality(H) + 1$

⟨4⟩1. $IsFiniteSet(H)$

BY ⟨1⟩2

⟨4⟩2. $Q = H \cup \{ym\}$

BY DEF Q

⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2, *FS_AddElement*

⟨3⟩ QED
BY ⟨3⟩1, ⟨1⟩2, ⟨1⟩3

⟨2⟩ QED

⟨3⟩1. $Cardinality(H) \in Nat$

BY ⟨1⟩2
⟨3⟩2. $Cardinality(Q) \in Nat$
BY ⟨1⟩3
⟨3⟩3. $k \in Nat$
BY ⟨1⟩1
⟨3⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨3⟩1, ⟨3⟩2, ⟨3⟩3
⟨1⟩7. $k \leq Cardinality(Q)$
⟨2⟩1. $Q \in$ SUBSET Y
⟨3⟩1. $Q \subseteq Cm$
BY ⟨1⟩3
⟨3⟩2. $Cm \subseteq Y$
BY ⟨1⟩1
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2
⟨2⟩2. $IsACover(Q, X, Leq)$
BY ⟨1⟩5
⟨2⟩3. $Cardinality(Q) \leq Cardinality(C)$
BY ⟨1⟩6, ⟨1⟩1, ⟨1⟩3 DEF k
⟨2⟩4. $\forall r \in$ SUBSET Y :
$\lor \neg \land IsACover(r, X, Leq)$
$\land (Cardinality(r) \leq Cardinality(C))$
$\lor (Cardinality(C) \leq Cardinality(r))$
⟨3⟩1. $IsAMinCover(C, X, Y, Leq)$
OBVIOUS
⟨3⟩ QED
BY ⟨3⟩1, *HaveCardAsCost*, *ProblemInput*, *MinCoverPropertiesCard*
⟨2⟩5. $Cardinality(C) \leq Cardinality(Q)$
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4
⟨2⟩ QED
BY ⟨2⟩5 DEF k
⟨1⟩ QED
BY ⟨1⟩1, ⟨1⟩3, ⟨1⟩6, ⟨1⟩7

If a minimal cover C refines a minimal cover Cm,
then no two elements $a, b \in Cm$ can cover the same element $y \in C$.

THEOREM $AtMostOneAbove \triangleq$
ASSUME
NEW C,
NEW $y \in C$,
NEW $a \in Cm$, NEW $b \in Cm$,
$\land IsAMinCover(Cm, X, Y, Leq)$
$\land IsAMinCover(C, X, Y, Leq)$

$\land$ $Refines(C,\ Cm,\ Leq)$
$\land$ $a \neq b$
$\land$ $Leq[y,\ a]$
$\land$ $Leq[y,\ b]$
PROVE
FALSE
PROOF
$\langle 1\rangle$ DEFINE
$S \triangleq C \setminus \{y\}$
$H \triangleq Hat(S,\ Cm,\ Leq)$
$Q \triangleq H \cup \{y\}$
$k \triangleq Cardinality(Cm)$
$\langle 1\rangle 1.$ $\land$ $C \in$ SUBSET Y
$\land$ $Cm \in$ SUBSET Y
$\langle 2\rangle 1.$ $\land$ $IsAMinCover(Cm,\ X,\ Y,\ Leq)$
$\land$ $IsAMinCover(C,\ X,\ Y,\ Leq)$
OBVIOUS
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1$, $MinCoverProperties$
$\langle 1\rangle 2.$ $\land$ $IsFiniteSet(C)$
$\land$ $IsFiniteSet(Cm)$
$\land$ $Cardinality(Cm) \in Nat$
$\langle 2\rangle 1.$ $IsFiniteSet(Y)$
BY $XYAreFiniteSets$
$\langle 2\rangle$ QED
BY $\langle 1\rangle 1$, $\langle 2\rangle 1$, FS_Subset, $FS\_CardinalityType$
$\langle 1\rangle 3.$ $\land$ $\forall\, u \in C \setminus \{y\} :\ \neg Leq[u,\ a]$
$\land$ $\forall\, u \in C \setminus \{y\} :\ \neg Leq[u,\ b]$
$\langle 2\rangle 1.$ ASSUME
NEW $r \in Cm$,
NEW $u \in C \setminus \{y\}$,
$Leq[y,\ r]$
PROVE
$\neg Leq[u,\ r]$
$\langle 3\rangle 1.$ SUFFICES
ASSUME $Leq[u,\ r]$
PROVE FALSE
BY $\langle 3\rangle 1$
$\langle 3\rangle 2.$ $u \neq y$
BY $\langle 2\rangle 1$
$\langle 3\rangle 3.$ $\land$ $IsAMinCover(Cm,\ X,\ Y,\ Leq)$
$\land$ $IsAMinCover(C,\ X,\ Y,\ Leq)$
$\land$ $Refines(C,\ Cm,\ Leq)$
OBVIOUS
$\langle 3\rangle$ QED *goal from* $\langle 3\rangle 1$

BY $\langle 2\rangle 1$, $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, *AtMostOneBelow*
$a \leftarrow y$, $b \leftarrow u$, $ym \leftarrow r$

$\langle 2\rangle 2$. $\wedge\ a \in Cm$
$\wedge\ b \in Cm$
OBVIOUS

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

$\langle 1\rangle 4$. $\wedge\ a \notin H$
$\wedge\ b \notin H$

$\langle 2\rangle 1$. $a \notin H$
$\langle 3\rangle 1$. SUFFICES
ASSUME $a \in H$
PROVE FALSE
BY $\langle 3\rangle 1$
$\langle 3\rangle 2$. PICK $u \in S : a = SomeAbove(u, Cm, Leq)$
BY $\langle 3\rangle 1$ DEF H, *Hat*
$\langle 3\rangle 3$. $u \in C$
BY $\langle 3\rangle 2$ DEF S
$\langle 3\rangle 4$. $\exists\, r \in Cm : Leq[u, r]$
$\langle 4\rangle 1$. *Refines*(C, Cm, Leq)
OBVIOUS
$\langle 4\rangle$ QED
BY $\langle 4\rangle 1$, $\langle 3\rangle 3$ DEF *Refines*
$\langle 3\rangle 5$. $Leq[u, a]$
$\langle 4\rangle 1$. $a = SomeAbove(u, Cm, Leq)$
BY $\langle 3\rangle 2$
$\langle 4\rangle$ QED
BY $\langle 4\rangle 1$, $\langle 3\rangle 4$ DEF *SomeAbove*
$\langle 3\rangle 6$. $\neg Leq[u, a]$
BY $\langle 1\rangle 3$, $\langle 3\rangle 2$ DEF S
$\langle 3\rangle$ QED
BY $\langle 3\rangle 5$, $\langle 3\rangle 6$

$\langle 2\rangle 2$. $b \notin H$
$\langle 3\rangle 1$. SUFFICES
ASSUME $b \in H$
PROVE FALSE
BY $\langle 3\rangle 1$
$\langle 3\rangle 2$. PICK $u \in S : b = SomeAbove(u, Cm, Leq)$
BY $\langle 3\rangle 1$ DEF H, *Hat*
$\langle 3\rangle 3$. $u \in C$
BY $\langle 3\rangle 2$ DEF S
$\langle 3\rangle 4$. $\exists\, r \in Cm : Leq[u, r]$
$\langle 4\rangle 1$. *Refines*(C, Cm, Leq)
OBVIOUS
$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 3\rangle 3$ DEF *Refines*

$\langle 3\rangle 5$. $Leq[u,\ b]$

$\langle 4\rangle 1$. $b = SomeAbove(u,\ Cm,\ Leq)$

BY $\langle 3\rangle 2$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 3\rangle 4$ DEF *SomeAbove*

$\langle 3\rangle 6$. $\neg Leq[u,\ b]$

BY $\langle 1\rangle 3$, $\langle 3\rangle 2$ DEF S

$\langle 3\rangle$ QED

BY $\langle 3\rangle 5$, $\langle 3\rangle 6$

$\langle 2\rangle$ QED

BY $\langle 2\rangle 1$, $\langle 2\rangle 2$

$\langle 1\rangle 5$. $\land\ H \in$ SUBSET Cm
$\land\ Refines(S,\ H,\ Leq)$
$\land\ Cardinality(H) \leq Cardinality(S)$

$\langle 2\rangle 1$. $\land\ S \subseteq Z$
$\land\ Cm \subseteq Z$

$\langle 3\rangle 1$. $S \subseteq Z$

$\langle 4\rangle 1$. $S \subseteq C$

BY DEF S

$\langle 4\rangle 2$. $C \subseteq Y$

BY $\langle 1\rangle 1$

$\langle 4\rangle 3$. $Y \subseteq Z$

BY *ProblemInput*

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$

$\langle 3\rangle 2$. $Cm \subseteq Z$

$\langle 4\rangle 1$. $Cm \subseteq Y$

BY $\langle 1\rangle 1$

$\langle 4\rangle 2$. $Y \subseteq Z$

BY *ProblemInput*

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$

$\langle 3\rangle$ QED

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

$\langle 2\rangle 2$. $Refines(S,\ Cm,\ Leq)$

$\langle 3\rangle 1$. $S \subseteq C$

BY DEF S

$\langle 3\rangle 2$. $Refines(C,\ Cm,\ Leq)$

OBVIOUS

$\langle 3\rangle$ QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, *SubsetRefinesToo*
$S \leftarrow C,\ T \leftarrow Cm,\ R \leftarrow S$

$\langle 2\rangle$ QED

BY $\langle 2\rangle 1$, $\langle 2\rangle 2$, *HasHat* DEF H $T \leftarrow Cm$

⟨1⟩6. $\land\ IsFiniteSet(H)$
$\land\ Cardinality(H) \in Nat$
$\land\ Cardinality(H) \leq k - 2$
⟨2⟩1. $H \subseteq Cm \setminus \{a,\ b\}$
BY ⟨1⟩5, ⟨1⟩4
⟨2⟩2. $\land\ IsFiniteSet(Cm \setminus \{a,\ b\})$
$\land\ Cardinality(Cm \setminus \{a,\ b\}) = k - 2$
⟨3⟩1. $a \in Cm$
OBVIOUS
⟨3⟩2. $IsFiniteSet(Cm)$
BY ⟨1⟩2
⟨3⟩3. $\land\ IsFiniteSet(Cm \setminus \{a\})$
$\land\ Cardinality(Cm \setminus \{a\}) = Cardinality(Cm) - 1$
BY ⟨3⟩1, ⟨3⟩2, *FS_RemoveElement*
⟨3⟩4. $b \in (Cm \setminus \{a\})$
⟨4⟩1. $\land\ b \in Cm$
$\land\ a \neq b$
OBVIOUS
⟨4⟩ QED
BY ⟨4⟩1
⟨3⟩5. $\land\ IsFiniteSet(Cm \setminus \{a,\ b\})$
$\land\ Cardinality(Cm \setminus \{a,\ b\}) = Cardinality(Cm \setminus \{a\}) - 1$
BY ⟨3⟩3, ⟨3⟩4, *FS_RemoveElement*
⟨3⟩6. $Cardinality(Cm) \in Nat$
BY ⟨1⟩2
⟨3⟩ QED
BY ⟨3⟩3, ⟨3⟩5, ⟨3⟩6 DEF k
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, *FS_Subset*, *FS_CardinalityType*
⟨1⟩7. $IsACover(Q,\ C,\ Leq)$
⟨2⟩1. SUFFICES
ASSUME NEW $u \in C$
PROVE $\exists\, v \in Q :\ Leq[u,\ v]$
BY ⟨2⟩1 DEF *IsACover*
⟨2⟩2.CASE $u = y$
⟨3⟩ DEFINE $v \triangleq y$
⟨3⟩1. $v \in Q$
⟨4⟩1. $v \in H \cup \{y\}$
BY DEF v
⟨4⟩ QED
BY ⟨4⟩1 DEF Q
⟨3⟩2. $Leq[u,\ v]$
⟨4⟩1. $Leq[y,\ y]$
⟨5⟩1. $y \in Z$
⟨6⟩1. $y \in C$

OBVIOUS

⟨6⟩2. $C \subseteq Y$

BY ⟨1⟩1

⟨6⟩3. $Y \subseteq Z$

BY *ProblemInput*

⟨6⟩ QED

BY ⟨6⟩1, ⟨6⟩2, ⟨6⟩3

⟨5⟩2. *IsReflexive*(*Leq*)

BY *ProblemInput* DEF *IsACompleteLattice*, *IsAPartialOrder*

⟨5⟩ QED

BY ⟨5⟩1, ⟨5⟩2 DEF *IsReflexive*, *Z*

⟨4⟩ QED

BY ⟨4⟩1, ⟨2⟩2 DEF *v*

⟨3⟩ QED *goal from ⟨2⟩1*

BY ⟨3⟩1, ⟨3⟩2

⟨2⟩3. CASE $u \neq y$

⟨3⟩1. $u \in C \setminus \{y\}$

BY ⟨2⟩1, ⟨2⟩3

⟨3⟩2. $u \in S$

BY ⟨3⟩1 DEF *S*

⟨3⟩3. *Refines*(*S*, *H*, *Leq*)

BY ⟨1⟩5

⟨3⟩4. $\forall\, p \in S : \exists\, q \in H : Leq[p, q]$

BY ⟨3⟩3 DEF *Refines*

⟨3⟩5. PICK $v \in H : Leq[u, v]$

BY ⟨3⟩4, ⟨3⟩2

⟨3⟩6. $v \in Q$

BY ⟨3⟩5 DEF *Q*

⟨3⟩ QED *goal from ⟨2⟩1*

BY ⟨3⟩5, ⟨3⟩5

⟨2⟩ QED

BY ⟨2⟩2, ⟨2⟩3

⟨1⟩8. *IsACover*(*Q*, *X*, *Leq*)

⟨2⟩1. *IsACover*(*Q*, *C*, *Leq*)

BY ⟨1⟩7

⟨2⟩2. *IsACover*(*C*, *X*, *Leq*)

⟨3⟩1. *IsAMinCover*(*C*, *X*, *Y*, *Leq*)

OBVIOUS

⟨3⟩ QED

BY ⟨3⟩1, *MinCoverProperties*

⟨2⟩3. *IsTransitive*(*Leq*)

BY *ProblemInput* DEF *IsACompleteLattice*, *IsAPartialOrder*

⟨2⟩4. $\wedge\, X \subseteq Z$

$\wedge\, C \subseteq Z$

$\wedge\ Q \subseteq Z$
⟨3⟩1. $X \subseteq Z$
BY *ProblemInput*
⟨3⟩2. $C \subseteq Z$
⟨4⟩1. $C \subseteq Y$
BY ⟨1⟩1
⟨4⟩2. $Y \subseteq Z$
BY *ProblemInput*
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2
⟨3⟩3. $Q \subseteq Z$
⟨4⟩1. $Q = H \cup \{y\}$
BY DEF Q
⟨4⟩2. $Y \subseteq Z$
BY *ProblemInput*
⟨4⟩3. $H \subseteq Z$
⟨5⟩1. $H \subseteq Cm$
BY ⟨1⟩5
⟨5⟩2. $Cm \subseteq Y$
BY ⟨1⟩1
⟨5⟩ QED
BY ⟨5⟩1, ⟨5⟩2, ⟨4⟩2
⟨4⟩4. $y \in Z$
⟨5⟩1. $y \in C$
OBVIOUS
⟨5⟩2. $C \subseteq Y$
BY ⟨1⟩1
⟨5⟩ QED
BY ⟨5⟩1, ⟨5⟩2, ⟨4⟩2
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩3, ⟨4⟩4
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, *CoveringIsTransitive* DEF Z
$A \leftarrow X,\ B \leftarrow C,\ C \leftarrow Q$
⟨1⟩9. $\wedge$ *IsFiniteSet*(Q)
$\wedge$ *Cardinality*$(Q) \in Nat$
$\wedge$ *Cardinality*$(Q) \leq k - 1$
⟨2⟩1. $\wedge$ *IsFiniteSet*(Q)
$\wedge$ *Cardinality*$(Q) \leq$ *Cardinality*$(H) + 1$
⟨3⟩1. *IsFiniteSet*(H)
BY ⟨1⟩6
⟨3⟩2. $Q = H \cup \{y\}$
BY DEF Q

⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, *FS_AddElementUpperBound*
⟨2⟩2. ∧ $Cardinality(H) \in Nat$
∧ $Cardinality(H) \leq k - 2$
BY ⟨1⟩6
⟨2⟩3. $k \in Nat$
BY ⟨1⟩2 DEF k
⟨2⟩4. $Cardinality(Q) \in Nat$
BY ⟨2⟩1, *FS_CardinalityType*
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4
⟨1⟩10. $k \leq Cardinality(Q)$
⟨2⟩1. $Q \in$ SUBSET Y
⟨3⟩1. $Q = H \cup \{y\}$
BY DEF Q
⟨3⟩2. $H \subseteq Y$
⟨4⟩1. $H \subseteq Cm$
BY ⟨1⟩5
⟨4⟩2. $Cm \subseteq Y$
BY ⟨1⟩1
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2
⟨3⟩3. $y \in Y$
⟨4⟩1. $y \in C$
OBVIOUS
⟨4⟩2. $C \subseteq Y$
⟨5⟩1. $IsAMinCover(C, X, Y, Leq)$
OBVIOUS
⟨5⟩ QED
BY ⟨5⟩1, *MinCoverProperties*
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3
⟨2⟩2. $IsACover(Q, X, Leq)$
BY ⟨1⟩8
⟨2⟩3. $Cardinality(Q) \leq Cardinality(Cm)$
⟨3⟩1. $Cardinality(Q) \in Nat$
BY ⟨1⟩9
⟨3⟩2. $Cardinality(Cm) \in Nat$
BY ⟨1⟩2
⟨3⟩3. $Cardinality(Q) \leq k - 1$
BY ⟨1⟩9
⟨3⟩4. $k = Cardinality(Cm)$
BY DEF k

⟨3⟩ QED
BY ⟨2⟩1, ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4
⟨2⟩4. ∀ $r \in$ SUBSET Y :
$\lor \neg \land IsACover(r, X, Leq)$
$\land Cardinality(r) \leq Cardinality(Cm)$
$\lor Cardinality(Cm) \leq Cardinality(r)$
⟨3⟩1. $IsAMinCover(Cm, X, Y, Leq)$
OBVIOUS
⟨3⟩ QED
BY ⟨3⟩1, $HaveCardAsCost$, $ProblemInput$, $MinCoverPropertiesCard$
⟨2⟩5. $Cardinality(Cm) \leq Cardinality(Q)$
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4
⟨2⟩ QED
BY ⟨2⟩5 DEF k
⟨1⟩ QED
⟨2⟩1. $\land Cardinality(Q) \in Nat$
$\land k \in Nat$
BY ⟨1⟩9, ⟨1⟩2 DEF k
⟨2⟩2. $Cardinality(Q) \leq k - 1$
BY ⟨1⟩9
⟨2⟩3. $k \leq Cardinality(Q)$
BY ⟨1⟩10
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3

If a minimal cover C refines another minimal cover Cm, then Leq induces a unique bijection between them.

THEOREM $MinCoverRefinementInducesBijection \triangleq$
ASSUME
NEW C,
$\land IsAMinCover(C, X, Y, Leq)$
$\land IsAMinCover(Cm, X, Y, Leq)$
$\land Refines(C, Cm, Leq)$
PROVE
LET $g \triangleq LeqToBij(C)$
IN $\land g \in Bijection(1 \,..\, N, C)$
$\land \forall q \in 1 \,..\, N :$
$\land Leq[g[q], Lm[q]]$
$\land \forall p \in 1 \,..\, N \setminus \{q\} :$
$Lm[q]$is above only $g[q]$
$\land \neg Leq[g[p], Lm[q]]$
$g[q]$is below only $Lm[q]$
$\land \neg Leq[g[q], Lm[p]]$

PROOF
⟨1⟩ DEFINE
  $g \triangleq LeqToBij(C)$
  $f \triangleq [ym \in Cm \mapsto \text{CHOOSE } y \in C : Leq[y, ym]]$
  $h \triangleq [q \in 1 \,..\, N \mapsto f[Lm[q]]]$
  $R \triangleq Range(h)$
⟨1⟩1. $\wedge IsAMinCover(C, X, Y, Leq)$
    $\wedge IsAMinCover(Cm, X, Y, Leq)$
    $\wedge Refines(C, Cm, Leq)$
    $\wedge C \in \text{SUBSET } Y$
    $\wedge IsACover(C, X, Leq)$
    $\wedge Cm \in \text{SUBSET } Y$
  ⟨2⟩1. $\wedge IsAMinCover(Cm, X, Y, Leq)$
      $\wedge IsAMinCover(C, X, Y, Leq)$
      $\wedge Refines(C, Cm, Leq)$
    OBVIOUS
  ⟨2⟩2. $\wedge C \in \text{SUBSET } Y$
      $\wedge IsACover(C, X, Leq)$
    BY ⟨2⟩1, *MinCoverProperties*
  ⟨2⟩3. $\wedge Cm \in \text{SUBSET } Y$
    BY ⟨2⟩1, *MinCoverProperties*
  ⟨2⟩ QED
    BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3
⟨1⟩2. $\forall ym \in Cm : \wedge f[ym] \in C$
                $\wedge Leq[f[ym], ym]$
  ⟨2⟩1. SUFFICES ASSUME NEW $ym \in Cm$
          PROVE $\wedge f[ym] \in C$
                $\wedge Leq[f[ym], ym]$
    BY ⟨2⟩1
  ⟨2⟩2. $f[ym] = \text{CHOOSE } y \in C : Leq[y, ym]$
    ⟨3⟩1. $ym \in \text{DOMAIN } f$
      ⟨4⟩1. $ym \in Cm$
        BY ⟨2⟩1
      ⟨4⟩2. $Cm = \text{DOMAIN } f$
        BY DEF f
      ⟨4⟩ QED
        BY ⟨4⟩1, ⟨4⟩2
    ⟨3⟩ QED
      BY ⟨3⟩1 DEF f
  ⟨2⟩3. $\forall yq \in Cm : \exists y \in C : Leq[y, yq]$
    BY ⟨1⟩1, *MinCoverRefinementHasBelow*
  ⟨2⟩4. $\exists y \in C : Leq[y, ym]$
    ⟨3⟩1. $ym \in Cm$
      BY ⟨2⟩1
    ⟨3⟩ QED

BY $\langle 2\rangle 3$, $\langle 3\rangle 1$ $yq \leftarrow ym$

$\langle 2\rangle$ QED *goal from* $\langle 2\rangle 1$

BY $\langle 2\rangle 2$, $\langle 2\rangle 4$

$\langle 1\rangle 3.\ \wedge\ h \in \mathit{Bijection}(1\,..\,N,\ C)$
$\quad\wedge\ \forall\, q \in 1\,..\,N :\ \mathit{Leq}[h[q],\ \mathit{Lm}[q]]$

$\langle 2\rangle 1.\ h \in [1\,..\,N \to C]$

$\langle 3\rangle 1.$ ASSUME NEW $q \in 1\,..\,N$
PROVE $h[q] \in C$

$\langle 4\rangle$ DEFINE
$ym \triangleq \mathit{Lm}[q]$
$y \triangleq f[ym]$

$\langle 4\rangle 1.\ \mathit{Lm} \in [1\,..\,N \to \mathit{Cm}]$
BY $\langle 1\rangle 1$, *LmIsBijection* DEF *Bijection*, *Injection*

$\langle 4\rangle 2.\ ym \in \mathit{Cm}$
BY $\langle 4\rangle 1$, $\langle 3\rangle 1$ DEF ym

$\langle 4\rangle 3.\ y \in C$

$\langle 5\rangle 1.\ f[ym] \in C$
BY $\langle 1\rangle 2$, $\langle 4\rangle 2$

$\langle 5\rangle$ QED
BY $\langle 5\rangle 1$ DEF y

$\langle 4\rangle 4.\ h[q] = y$

$\langle 5\rangle 1.\ h[q] = f[\mathit{Lm}[q]]$
BY $\langle 3\rangle 1$ DEF h

$\langle 5\rangle 2.\ h[q] = f[ym]$
BY $\langle 5\rangle 1$ DEF ym

$\langle 5\rangle$ QED
BY $\langle 5\rangle 2$ DEF y

$\langle 4\rangle$ QED
BY $\langle 4\rangle 3$, $\langle 4\rangle 4$

$\langle 3\rangle$ QED
BY $\langle 3\rangle 1$ DEF h

$\langle 2\rangle 2.\ h \in \mathit{Injection}(1\,..\,N,\ C)$

$\langle 3\rangle 1.$ SUFFICES
ASSUME
NEW $qa \in 1\,..\,N$, NEW $qb \in 1\,..\,N$,
$\wedge\ qa \neq qb$
$\wedge\ h[qa] = h[qb]$
PROVE FALSE
BY $\langle 3\rangle 1$, $\langle 2\rangle 1$ DEF *Injection*

$\langle 3\rangle 2.\ \wedge\ h[qa] = f[\mathit{Lm}[qa]]$
$\quad\wedge\ h[qb] = f[\mathit{Lm}[qb]]$
BY $\langle 3\rangle 1$ DEF h

$\langle 3\rangle$ DEFINE
$a \triangleq \mathit{Lm}[qa]$
$b \triangleq \mathit{Lm}[qb]$

$y \triangleq f[a]$

⟨3⟩3. $y = f[b]$

⟨4⟩1. $h[qa] = h[qb]$

BY ⟨3⟩1

⟨4⟩2. $f[Lm[qa]] = f[Lm[qb]]$

BY ⟨4⟩1, ⟨3⟩2

⟨4⟩3. $f[a] = f[b]$

BY ⟨4⟩2 DEF a, b

⟨4⟩ QED

BY ⟨4⟩3 DEF y

⟨3⟩4. $\land\ a \neq b$
$\land\ y \in C$
$\land\ a \in Cm$
$\land\ b \in Cm$
$\land\ Leq[y,\ a] \land Leq[y,\ b]$

⟨4⟩1. $\land\ Lm \in [1\ldots N \to Cm]$
$\land\ \forall\, a1,\ b1 \in 1\ldots N :$
$(Lm[a1] = Lm[b1]) \Rightarrow (a1 = b1)$

BY ⟨1⟩1, *LmIsBijection* DEF *Bijection*, *Injection*
$M \leftarrow Lm,\ S \leftarrow 1\ldots N,\ T \leftarrow Cm$

⟨4⟩2. $\land\ qa \in 1\ldots N$
$\land\ qb \in 1\ldots N$
$\land\ qa \neq qb$

BY ⟨3⟩1

⟨4⟩3. $a \neq b$

⟨5⟩1. $Lm[qa] \neq Lm[qb]$

BY ⟨4⟩1, ⟨4⟩2

⟨5⟩ QED

BY ⟨5⟩1 DEF a, b

⟨4⟩4. $\land\ y \in C$
$\land\ a \in Cm$
$\land\ b \in Cm$
$\land\ Leq[y,\ a] \land Leq[y,\ b]$

⟨5⟩1. $\land\ a \in Cm$
$\land\ b \in Cm$

⟨6⟩1. $\land\ Lm[qa] \in Cm$
$\land\ Lm[qb] \in Cm$

BY ⟨4⟩1, ⟨4⟩2

⟨6⟩ QED

BY ⟨6⟩1 DEF a, b

⟨5⟩2. $\land\ f[a] \in C$
$\land\ Leq[f[a],\ a]$
$\land\ Leq[f[b],\ b]$

BY ⟨1⟩2, ⟨5⟩1

⟨5⟩3. $\land\ y \in C$

$\wedge\ Leq[y,\ a]$
$\wedge\ Leq[y,\ b]$
BY $\langle 5\rangle 2$, $\langle 3\rangle 3$ DEF y
$\langle 5\rangle$ QED
BY $\langle 5\rangle 1$, $\langle 5\rangle 3$
$\langle 4\rangle$ QED
BY $\langle 4\rangle 3$, $\langle 4\rangle 4$
$\langle 3\rangle$ QED *goal from* $\langle 3\rangle 1$
BY $\langle 3\rangle 4$, $\langle 1\rangle 1$, *AtMostOneAbove*

$\langle 2\rangle 3.\ h \in Surjection(1\ldots N,\ C)$
An alternative proof for this step is via AtMostOneBelow
$\langle 3\rangle 1.$ SUFFICES
ASSUME NEW $t \in C$,
$\forall\, s \in 1\ldots N :\ h[s] \neq t$
PROVE FALSE
BY $\langle 3\rangle 1$, $\langle 2\rangle 1$ DEF *Surjection*
$\langle 3\rangle 2.\ h \in Injection(1\ldots N,\ C)$
BY $\langle 2\rangle 2$
$\langle 3\rangle 3.\ \wedge\ R \subseteq C$
$\wedge\ R \neq C$
$\langle 4\rangle 1.\ R \subseteq C$
BY $\langle 3\rangle 2$ DEF R, *Range*, *Injection*
$\langle 4\rangle 2.\ t \notin R$
$\langle 5\rangle 1.$ SUFFICES
ASSUME $t \in R$
PROVE FALSE
BY $\langle 5\rangle 1$
$\langle 5\rangle 2.$ PICK $s \in 1\ldots N :\ h[s] = t$
$\langle 6\rangle 1.\ h \in [1\ldots N \to C]$
BY $\langle 3\rangle 2$ DEF *Injection*
$\langle 6\rangle 2.\ (\text{DOMAIN}\ h) = (1\ldots N)$
BY $\langle 6\rangle 1$
$\langle 6\rangle 3.\ t \in \{h[x] :\ x \in \text{DOMAIN}\ h\}$
BY $\langle 5\rangle 1$ DEF R, *Range*
$\langle 6\rangle 4.\ t \in \{h[x] :\ x \in 1\ldots N\}$
BY $\langle 6\rangle 2$, $\langle 6\rangle 3$
$\langle 6\rangle$ QED
BY $\langle 6\rangle 4$
$\langle 5\rangle$ QED *goal from* $\langle 5\rangle 1$
BY $\langle 5\rangle 2$, $\langle 3\rangle 1$
$\langle 4\rangle$ QED
BY $\langle 4\rangle 1$, $\langle 4\rangle 2$
$\langle 3\rangle 4.\ h \in Surjection(1\ldots N,\ R)$
h is a surjection on its range

BY $\langle 2\rangle 1$, *Fun_RangeProperties* DEF R
$f \leftarrow h,\ S \leftarrow 1 \,..\, N,\ T \leftarrow C$

$\langle 3\rangle 5.\ N \in Nat$

$\langle 4\rangle 1.\ N = Cardinality(Cm)$

BY DEF N

$\langle 4\rangle 2.\ IsFiniteSet(Cm)$

$\langle 5\rangle 1.\ Cm \in \text{SUBSET } Y$

BY $\langle 1\rangle 1$

$\langle 5\rangle 2.\ IsFiniteSet(Y)$

BY *XYAreFiniteSets*

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, *FS_Subset*

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, *FS_CardinalityType*

$\langle 3\rangle 6.\ \wedge\ IsFiniteSet(1 \,..\, N)$
$\quad \wedge\ Cardinality(1 \,..\, N) = N$

$\langle 4\rangle$ DEFINE $bij \triangleq [x \in 1 \,..\, N \mapsto x]$

$\langle 4\rangle 1.\ bij \in Bijection(1 \,..\, N,\ 1 \,..\, N)$

BY DEF bij, *Bijection*, *Injection*, *Surjection*

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 3\rangle 5$, *FS_NatBijection*, *FS_CountingElements*
DEF *ExistsBijection*

$\langle 3\rangle 7.\ \wedge\ IsFiniteSet(R)$
$\quad \wedge\ Cardinality(R) = N$

$\langle 4\rangle 1.\ h \in Injection(1 \,..\, N,\ R)$

BY $\langle 3\rangle 2$, $\langle 3\rangle 4$ DEF *Surjection*, *Injection*

$\langle 4\rangle$ QED

BY $\langle 3\rangle 4$, $\langle 3\rangle 6$, $\langle 4\rangle 1$, *FS_Surjection*
$S \leftarrow 1 \,..\, N,\ T \leftarrow R$

$\langle 3\rangle 8.\ Cardinality(R) < N$

$\langle 4\rangle 1.\ IsFiniteSet(C)$

$\langle 5\rangle 1.\ C \in \text{SUBSET } Y$

BY $\langle 1\rangle 1$

$\langle 5\rangle 2.\ IsFiniteSet(Y)$

BY *XYAreFiniteSets*

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, *FS_Subset*

$\langle 4\rangle 2.\ Cardinality(R) < Cardinality(C)$

BY $\langle 4\rangle 1$, $\langle 3\rangle 3$, *FS_Subset*, *FS_CardinalityType*

$\langle 4\rangle 3.\ Cardinality(C) = N$

$\langle 5\rangle 1.\ N = Cardinality(Cm)$

BY DEF N

$\langle 5\rangle 2.\ Cardinality(C) = Cardinality(Cm)$

BY $\langle 1\rangle 1$, *AllMinCoversSameCard*,
HaveCardAsCost, *ProblemInput*,

⟨5⟩ QED
BY ⟨5⟩1, ⟨5⟩2
⟨4⟩ QED
BY ⟨4⟩2, ⟨4⟩3
⟨3⟩9. $\wedge\ Cardinality(R) \in Nat$
$\wedge\ Cardinality(R) < N$
$\wedge\ Cardinality(R) = N$
BY ⟨3⟩7, ⟨3⟩8, *FS_CardinalityType*
⟨3⟩ QED
BY ⟨3⟩9, ⟨3⟩5

⟨2⟩4. ASSUME NEW $q \in 1 \,..\, N$
PROVE $Leq[h[q], Lm[q]]$
⟨3⟩ DEFINE
$ym \triangleq Lm[q]$
$y \triangleq f[ym]$
⟨3⟩1. $h[q] = y$
⟨4⟩1. $h[q] = f[Lm[q]]$
⟨5⟩1. $q \in$ DOMAIN h
⟨6⟩1. $q \in 1 \,..\, N$
BY ⟨2⟩4
⟨6⟩2. (DOMAIN h) $= (1 \,..\, N)$
BY DEF h
⟨6⟩ QED
BY ⟨6⟩1, ⟨6⟩2
⟨5⟩ QED
BY ⟨5⟩1 DEF h
⟨4⟩ QED
BY ⟨4⟩1 DEF y, ym
⟨3⟩2. $Leq[y, ym]$
⟨4⟩1. $ym \in Cm$
⟨5⟩1. $q \in 1 \,..\, N$
BY ⟨2⟩4
⟨5⟩2. $Lm \in [1 \,..\, N \to Cm]$
BY ⟨1⟩1, *LmIsBijection* DEF *Bijection*, *Injection*
⟨5⟩3. $Lm[q] \in Cm$
BY ⟨5⟩1, ⟨5⟩2
⟨5⟩ QED
BY ⟨5⟩3 DEF ym
⟨4⟩2. $Leq[f[ym], ym]$
BY ⟨1⟩2, ⟨4⟩1
⟨4⟩ QED
BY ⟨4⟩2 DEF y
⟨3⟩ QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$ DEF ym

$\langle 2\rangle$ QED

BY $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 2\rangle 4$ DEF *Bijection*

$\langle 1\rangle 4$. $\land\ g \in \mathit{Bijection}(1\,..\,N,\ C)$
$\land\ \forall\, q \in 1\,..\,N :\ \mathit{Leq}[g[q],\ \mathit{Lm}[q]]$

BY $\langle 1\rangle 3$ DEF g, *LeqToBij*

$\langle 1\rangle 5$. ASSUME
NEW $q \in 1\,..\,N$,
NEW $p \in 1\,..\,N \setminus \{q\}$
PROVE
$\land \neg \mathit{Leq}[g[p],\ \mathit{Lm}[q]]$
$\land \neg \mathit{Leq}[g[q],\ \mathit{Lm}[p]]$

$\langle 2\rangle 1$. $\land\ p \neq q$
$\land\ p \in 1\,..\,N$
$\land\ q \in 1\,..\,N$

$\langle 3\rangle 1$. $p \neq q$

BY $\langle 1\rangle 5$

$\langle 3\rangle 2$. $\land\ p \in 1\,..\,N$
$\land\ q \in 1\,..\,N$

BY $\langle 1\rangle 5$

$\langle 3\rangle$ QED

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

$\langle 2\rangle 2$. $\mathit{Leq}[g[q],\ \mathit{Lm}[q]]$

BY $\langle 1\rangle 4$, $\langle 1\rangle 5$

$\langle 2\rangle 3$. ASSUME $\mathit{Leq}[g[p],\ \mathit{Lm}[q]]$
PROVE FALSE

$\langle 3\rangle$ DEFINE
$a \triangleq g[p]$
$b \triangleq g[q]$
$ym \triangleq \mathit{Lm}[q]$

$\langle 3\rangle 1$. $a \neq b$

$\langle 4\rangle 3$. $g \in \mathit{Bijection}(1\,..\,N,\ C)$

BY $\langle 1\rangle 4$

$\langle 4\rangle 4$. $g[p] \neq g[q]$

BY $\langle 2\rangle 1$, $\langle 4\rangle 3$ DEF *Bijection*, *Injection*

$\langle 4\rangle$ QED

BY $\langle 4\rangle 4$ DEF a, b

$\langle 3\rangle 2$. $\land\ \mathit{Leq}[a,\ ym]$
$\land\ \mathit{Leq}[b,\ ym]$

BY $\langle 2\rangle 3$, $\langle 2\rangle 2$ DEF a, b, ym

$\langle 3\rangle 3$. $\land\ a \in C$
$\land\ b \in C$
$\land\ ym \in Cm$

$\langle 4\rangle 1$. $\land\ a \in C$
$\land\ b \in C$

⟨5⟩1. $g \in [1 \,..\, N \to C]$
BY ⟨1⟩4 DEF *Bijection*, *Injection*
⟨5⟩2. $\land\ p \in 1 \,..\, N$
$\land\ q \in 1 \,..\, N$
BY ⟨1⟩5
⟨5⟩ QED
BY ⟨5⟩1, ⟨5⟩2 DEF a, b
⟨4⟩2. $ym \in Cm$
⟨5⟩1. $Lm \in [1 \,..\, N \to Cm]$
BY ⟨1⟩1, *LmIsBijection* DEF *Bijection*, *Injection*
⟨5⟩2. $q \in 1 \,..\, N$
BY ⟨1⟩5
⟨5⟩ QED
BY ⟨5⟩1, ⟨5⟩2 DEF ym
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2
⟨3⟩ QED
BY ⟨1⟩1, ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, *AtMostOneBelow*
⟨2⟩4. ASSUME $Leq[g[q], Lm[p]]$
PROVE FALSE
⟨3⟩ DEFINE
$a \triangleq Lm[p]$
$b \triangleq Lm[q]$
$y \triangleq g[q]$
⟨3⟩1. $a \neq b$
BY ⟨2⟩1, ⟨1⟩1, *LmIsBijection* DEF *Bijection*, *Injection*, a, b
⟨3⟩2. $\land\ Leq[y, a]$
$\land\ Leq[y, b]$
BY ⟨2⟩2, ⟨2⟩4 DEF a, b, y
⟨3⟩3. $\land\ a \in Cm$
$\land\ b \in Cm$
$\land\ y \in C$
⟨4⟩1. $\land\ a \in Cm$
$\land\ b \in Cm$
⟨5⟩1. $Lm \in [1 \,..\, N \to Cm]$
BY ⟨1⟩1, *LmIsBijection* DEF *Bijection*, *Injection*
⟨5⟩2. $\land\ Lm[p] \in Cm$
$\land\ Lm[q] \in Cm$
BY ⟨5⟩1, ⟨2⟩1
⟨5⟩ QED
BY ⟨5⟩2 DEF a, b
⟨4⟩2. $y \in C$
⟨5⟩1. $g \in [1 \,..\, N \to C]$
BY ⟨1⟩4 DEF *Bijection*, *Injection*
⟨5⟩2. $g[q] \in C$

```
                BY ⟨5⟩1, ⟨2⟩1
            ⟨5⟩ QED
                BY ⟨5⟩2 DEF y
        ⟨4⟩ QED
            BY ⟨4⟩1, ⟨4⟩2
    ⟨3⟩ QED
        ⟨4⟩ QED
            BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨1⟩1, AtMostOneAbove
⟨2⟩ QED
    BY ⟨2⟩3, ⟨2⟩4
⟨1⟩ QED
    BY ⟨1⟩4, ⟨1⟩5 DEF g
```

Type formula for the operator more that appears in the definition in the definition of the action Expand

```
THEOREM MoreInSeqSubsetY ≜
    ASSUME
        ∧ TypeInv
        ∧ stack ≠ ⟨⟩
    PROVE
        LET
            end ≜ Len(stack)
            PartialCover ≜ stack[end]
            i ≜ Cardinality(PartialCover)
            k ≜ i + 1
            ymax ≜ Lm[k]
            Q ≜ PartialCover ∪ Patch(k)
            succ ≜ BelowAndSuff(ymax, Q, Y)
            enum ≜ Enumerate(succ)
            more ≜ [r ∈ 1 .. Len(enum) ↦ PartialCover ∪ {enum[r]}]
        IN
            more ∈ Seq(SUBSET Y)
PROOF
⟨1⟩ DEFINE
    S ≜ SUBSET Y
    end ≜ Len(stack)
    PartialCover ≜ stack[end]
    i ≜ Cardinality(PartialCover)
    k ≜ i + 1
    ymax ≜ Lm[k]
    Q ≜ PartialCover ∪ Patch(k)
    succ ≜ BelowAndSuff(ymax, Q, Y)
    enum ≜ Enumerate(succ)
    more ≜ [r ∈ 1 .. Len(enum) ↦ PartialCover ∪ {enum[r]}]
```

⟨1⟩ HIDE DEF S, end, $PartialCover$, i, k, $ymax$, Q, $succ$, $enum$, $more$
⟨1⟩1. SUFFICES $more \in Seq(S)$
BY ⟨1⟩1 DEF S, end, $PartialCover$, i, k, $ymax$, Q, $succ$, $enum$, $more$
⟨1⟩ DEFINE
$n \triangleq Len(enum)$
⟨1⟩2. $more = [r \in 1 \,..\, n \mapsto PartialCover \cup \{enum[r]\}]$
BY DEF $more$, n
⟨1⟩3. $IsFiniteSet(succ)$
⟨2⟩1. $IsFiniteSet(Y)$
BY $XYAreFiniteSets$
⟨2⟩ QED
BY ⟨2⟩1, $BelowAndSuffIsFinite$ DEF $succ$
⟨1⟩4. $n \in Nat$
⟨2⟩2. $Len(enum) \in Nat$
BY ⟨1⟩3, $EnumerateProperties$ DEF $enum$
⟨2⟩ QED
BY ⟨2⟩2 DEF n
⟨1⟩5. SUFFICES
ASSUME NEW $r \in 1 \,..\, n$
PROVE $(PartialCover \cup \{enum[r]\}) \in S$
⟨2⟩ DEFINE $F(r) \triangleq PartialCover \cup \{enum[r]\}$
⟨2⟩ HIDE DEF F
⟨2⟩1. $\forall\, r \in 1 \,..\, n :\ F(r) \in S$
BY ⟨1⟩5 DEF F
⟨2⟩2. $[r \in 1 \,..\, n \mapsto F(r)] \in Seq(S)$
BY ⟨2⟩1, ⟨1⟩4, $IsASeq$
⟨2⟩ QED *goal from* ⟨1⟩1
BY ⟨2⟩2, ⟨1⟩2 DEF F
⟨1⟩6. $succ \subseteq Y$
BY DEF $succ$, $BelowAndSuff$
⟨1⟩7. $enum \in Bijection(1 \,..\, n, succ)$
BY ⟨1⟩3, $EnumerateProperties$ DEF $enum$, n
⟨1⟩8. $enum[r] \in succ$
BY ⟨1⟩5, ⟨1⟩7 DEF $Bijection$, $Injection$
⟨1⟩9. $enum[r] \in Y$
BY ⟨1⟩6, ⟨1⟩8
⟨1⟩10. $PartialCover \in$ SUBSET Y
⟨2⟩1. $TypeInv$
OBVIOUS
⟨2⟩2. $stack \in Seq(S)$
BY ⟨2⟩1 DEF $TypeInv$, S
⟨2⟩3. $\land\, end \in Nat$
$\land\, stack \in [1 \,..\, end \to S]$
$\land\, (\text{DOMAIN } stack) = (1 \,..\, end)$
BY ⟨2⟩2, $LenProperties$ DEF end

⟨2⟩4. $end \in (1 \,..\, end)$
BY ⟨2⟩3, $stack \neq \langle\rangle$ DEF end, $EmptySeq$
⟨2⟩5. $end \in (\text{DOMAIN } stack)$
BY ⟨2⟩3, ⟨2⟩4
⟨2⟩6. $stack[end] \in S$
BY ⟨2⟩3, ⟨2⟩5
⟨2⟩ QED
BY ⟨2⟩6 DEF $PartialCover$, S
⟨1⟩11. $(PartialCover \cup \{enum[r]\}) \in \text{SUBSET } Y$
BY ⟨1⟩9, ⟨1⟩10
⟨1⟩ QED *goal from ⟨1⟩5*
BY ⟨1⟩11 DEF S

Invariance theorems.

THEOREM $TypeOK \triangleq$
$Spec \Rightarrow \Box TypeInv$
PROOF
⟨1⟩1. ASSUME $Init$
PROVE $TypeInv$
⟨2⟩1. $\land\ stack = \langle\{\}\rangle$
$\land\ MinCoversBelow = \{\}$
BY ⟨1⟩1 DEF $Init$
⟨2⟩2. $stack \in Seq(\text{SUBSET } Y)$
⟨3⟩1. $stack \in [1 \,..\, 1 \to \text{SUBSET } Y]$
BY ⟨2⟩1
⟨3⟩ QED
BY ⟨3⟩1, $SeqDef$ DEF Seq
⟨2⟩3. $MinCoversBelow \subseteq \text{SUBSET } Y$
BY ⟨2⟩1
⟨2⟩ QED
BY ⟨2⟩2, ⟨2⟩3 DEF $TypeInv$
⟨1⟩2. ASSUME $TypeInv \land Next$
PROVE $TypeInv'$
⟨2⟩ DEFINE
$end \triangleq Len(stack)$
$Partial \triangleq stack[end]$
$i \triangleq Cardinality(Partial)$
$k \triangleq i + 1$
$front \triangleq SubSeq(stack, 1, end - 1)$
$ymax \triangleq Lm[k]$
$Q \triangleq Partial \cup Patch(k)$
$succ \triangleq BelowAndSuff(ymax, Q, Y)$
$enum \triangleq Enumerate(succ)$

$more \triangleq [r \in 1 \,..\, Len(enum) \mapsto Partial \cup \{enum[r]\}]$

⟨2⟩1. $\wedge\ stack \in Seq(\text{SUBSET } Y)$
$\wedge\ MinCoversBelow \subseteq \text{SUBSET } Y$
BY ⟨1⟩2 DEF *TypeInv*, *Next*

⟨2⟩2. SUFFICES $\wedge\ stack' \in Seq(\text{SUBSET } Y)$
$\wedge\ MinCoversBelow' \subseteq \text{SUBSET } Y$
BY ⟨2⟩2 DEF *TypeInv*

⟨2⟩3. $front \in Seq(\text{SUBSET } Y)$
BY ⟨2⟩1, *FrontProperties* DEF *Front*

⟨2⟩4. $more \in Seq(\text{SUBSET } Y)$
BY ⟨1⟩2, *MoreInSeqSubsetY* DEF *Next*

⟨2⟩5. CASE *Collect*

⟨3⟩1. $stack' \in Seq(\text{SUBSET } Y)$
BY ⟨2⟩5, ⟨2⟩3 DEF *Collect*

⟨3⟩2. $MinCoversBelow' \subseteq \text{SUBSET } Y$

⟨4⟩1. SUFFICES $Partial \in \text{SUBSET } Y$
BY ⟨2⟩1, ⟨4⟩1, ⟨2⟩5 DEF *Collect*

⟨4⟩2. $end \in 1 \,..\, end$

⟨5⟩1. $end \in Nat$
BY ⟨2⟩1, *LenProperties*

⟨5⟩2. $end \neq 0$
BY ⟨2⟩1, ⟨1⟩2, *EmptySeq* DEF *Next*

⟨5⟩ QED
BY ⟨5⟩1, ⟨5⟩2

⟨4⟩ QED
BY ⟨2⟩1, ⟨4⟩2, *ElementOfSeq*

⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2

⟨2⟩6. CASE *Expand*

⟨3⟩1. $stack' \in Seq(\text{SUBSET } Y)$
BY ⟨2⟩6, ⟨2⟩3, ⟨2⟩4, *ConcatProperties* DEF *Expand*

⟨3⟩2. $MinCoversBelow' \subseteq \text{SUBSET } Y$
BY ⟨2⟩1, ⟨2⟩6 DEF *Expand*

⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2

⟨2⟩ QED
BY ⟨2⟩5, ⟨2⟩6, ⟨1⟩2 DEF *Next*

⟨1⟩ DEFINE
$Nx \triangleq Next$

⟨1⟩3. ASSUME $TypeInv \wedge [Nx]_{vars}$
PROVE $TypeInv'$
BY ⟨1⟩2, ⟨1⟩3 DEF *TypeInv*, *vars*

⟨1⟩ QED

⟨2⟩1. $(TypeInv \wedge \Box[Nx]_{vars}) \Rightarrow \Box\, TypeInv$
BY ⟨1⟩3, *PTL*

⟨2⟩2. $(Init \wedge \Box[Next]_{vars}) \Rightarrow \Box TypeInv$
BY ⟨2⟩1, ⟨1⟩1
⟨2⟩ QED
BY ⟨2⟩2, *PTL* DEF *Spec*

We now show that :

$MinCoversOf(X,\ Y,\ Leq) \subseteq \text{UNION}\ \{$
$MinCoversBelow(Cm) : Cm \in MinCoversOf(X,\ Maxima(Y,\ Leq),\ Leq)\}$

Note that upon termination $Len(stack) = 0$

THEOREM $StrongReductionCompleteness \triangleq$
ASSUME
NEW $C \in \text{SUBSET}\ Y$,
The assumption $C \in AllCandidatesBelow(Cm,\ Y)$,
too, implies this domain formula.
$\wedge\ IsAMinCover(Cm,\ X,\ Max,\ Leq)$
$\wedge\ C \in AllCandidatesBelow(Cm,\ Y)$
PROVE
$Spec \Rightarrow \Box InvCompl(C)$
PROOF
⟨1⟩ DEFINE
$g \triangleq LeqToBij(C)$
$end \triangleq Len(stack)$
$PartialCover \triangleq stack[end]$
$i \triangleq Cardinality(PartialCover)$
$k \triangleq i + 1$
$front \triangleq SubSeq(stack,\ 1,\ end - 1)$

$y \triangleq g[k]$
$ymax \triangleq Lm[k]$
$Q \triangleq PartialCover \cup Patch(k)$
$succ \triangleq BelowAndSuff(ymax,\ Q,\ Y)$
$enum \triangleq Enumerate(succ)$
$more \triangleq [r \in 1\ ..\ Len(enum) \mapsto PartialCover \cup \{enum[r]\}]$
$After \triangleq \{g[t] :\ t \in (k+1)\ ..\ N\}$

⟨1⟩ HIDE DEF $g,\ end,\ i,\ PartialCover,\ k,\ front,$
$y,\ ymax,\ Q,\ succ,\ enum,\ more,\ After$

⟨1⟩1. ASSUME *Init*
PROVE $InvCompl(C)$
⟨2⟩1. $stack = \langle\{\}\rangle$
BY ⟨1⟩1 DEF *Init*
⟨2⟩2. $end = 1$
BY ⟨2⟩1 DEF *Len*, *end*

⟨2⟩3. ∧ $i = 0$
∧ $PartialCover = \{\}$
⟨3⟩1. $PartialCover = \{\}$
BY ⟨2⟩1, ⟨2⟩2 DEF $PartialCover$
⟨3⟩2. $i = 0$
BY ⟨3⟩1, $FS\_EmptySet$ DEF i
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2
⟨2⟩4. ∃ $t \in$ DOMAIN $stack$: $IsPrefixCov(stack[t], g)$
⟨3⟩1. $end \in$ DOMAIN $stack$
BY ⟨2⟩1, ⟨2⟩2
⟨3⟩2. $IsPrefixCov(PartialCover, g)$
⟨4⟩1. $PartialCover = \{g[q] : q \in 1 \,..\, i\}$
BY ⟨2⟩3
⟨4⟩ QED
BY ⟨4⟩1 DEF $IsPrefixCov$, i
⟨3⟩3. $PartialCover = stack[end]$
BY DEF $PartialCover$
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3
⟨2⟩ QED
BY ⟨2⟩4 DEF g, $InvCompl$

⟨1⟩2. ∧ $Cm \subseteq Y$
∧ $Cm \subseteq Max$
⟨2⟩1. $Cm \subseteq Maxima(Y, Leq)$
⟨3⟩1. $IsAMinCover(Cm, X, Max, Leq)$
OBVIOUS
⟨3⟩ QED
BY ⟨3⟩1, $MinCoverProperties$ DEF Max
⟨2⟩ QED
BY ⟨2⟩1, $MaxIsSubset$ DEF Max

⟨1⟩3. ASSUME $TypeInv \land TypeInv' \land Next \land InvCompl(C)$
PROVE $InvCompl(C)'$
⟨2⟩1. $N \in Nat$
⟨3⟩1. $N = Cardinality(Cm)$
BY DEF N
⟨3⟩2. $Cardinality(Cm) \in Nat$
⟨4⟩2. $Y \subseteq Z$
BY $ProblemInput$
⟨4⟩3. $Cm \subseteq Z$
BY ⟨1⟩2, ⟨4⟩2
⟨4⟩4. $IsFiniteSet(Z)$
BY $ProblemInput$

⟨4⟩ QED
BY ⟨4⟩3, ⟨4⟩4, *FS_Subset*, *FS_CardinalityType*
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2
⟨2⟩2. SUFFICES
ASSUME *IsAMinCover*(*C*, *X*, *Y*, *Leq*)
PROVE
$\lor \exists\, n \in \text{DOMAIN } stack' : IsPrefixCov(stack[n]', g)$
$\lor C \in MinCoversBelow'$
⟨3⟩1. $InvCompl(C)'$
$\equiv \lor \exists\, n \in \text{DOMAIN } stack' : IsPrefixCov(stack[n]', g)$
$\lor \neg IsAMinCover(C, X, Y, Leq)$
$\lor C \in MinCoversBelow'$
BY DEF *InvCompl*, *IsPrefixCov*, *g*,
IsAMinCover, *CoversOf*, *IsMinimal*, *IsACover*
⟨3⟩2. $\lor \exists\, n \in \text{DOMAIN } stack' : IsPrefixCov(stack[n]', g)$
$\lor \neg IsAMinCover(C, X, Y, Leq)$
$\lor C \in MinCoversBelow'$
BY ⟨2⟩2
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2
⟨2⟩3. $\lor \exists\, n \in \text{DOMAIN } stack : IsPrefixCov(stack[n], g)$
$\lor C \in MinCoversBelow$
⟨3⟩1. $InvCompl(C)$
BY ⟨1⟩3
⟨3⟩2. $\lor \exists\, n \in \text{DOMAIN } stack : IsPrefixCov(stack[n], g)$
$\lor \neg IsAMinCover(C, X, Y, Leq)$
$\lor C \in MinCoversBelow$
BY ⟨3⟩1 DEF *InvCompl*, *g*
⟨3⟩ QED
BY ⟨3⟩2, ⟨2⟩2
⟨2⟩4. ASSUME $C \in MinCoversBelow$
PROVE $C \in MinCoversBelow'$
⟨3⟩1. $\land\, stack \neq \langle\rangle$
$\land\, \lor Collect$
$\lor Expand$
BY ⟨1⟩3 DEF *Next*
⟨3⟩2. $MinCoversBelow \subseteq MinCoversBelow'$
⟨4⟩1. ASSUME *Collect*
PROVE $MinCoversBelow \subseteq MinCoversBelow'$
BY ⟨4⟩1 DEF *Collect*
⟨4⟩2. ASSUME *Expand*
PROVE $MinCoversBelow \subseteq MinCoversBelow'$
⟨5⟩1. UNCHANGED *MinCoversBelow*
BY ⟨4⟩2 DEF *Expand*

⟨5⟩ QED
BY ⟨5⟩1
⟨4⟩ QED
BY ⟨3⟩1, ⟨4⟩1, ⟨4⟩2
⟨3⟩ QED
BY ⟨2⟩4, ⟨3⟩2

⟨2⟩5. SUFFICES
ASSUME $C \notin MinCoversBelow$
PROVE
$\lor \exists\, n \in \text{DOMAIN } stack' : IsPrefixCov(stack[n]', g)$
$\lor C \in MinCoversBelow'$
⟨3⟩1. ASSUME $C \in MinCoversBelow$
PROVE $\lor \exists\, n \in \text{DOMAIN } stack' : IsPrefixCov(stack[n]', g)$
$\lor C \in MinCoversBelow'$
BY ⟨2⟩4
⟨3⟩ QED
BY ⟨2⟩5, ⟨3⟩1 *which are exhaustive cases*

⟨2⟩6. $\land stack \in Seq(\text{SUBSET } Y)$
$\land stack \in [1 \,..\, Len(stack) \to \text{SUBSET } Y]$
$\land (\text{DOMAIN } stack) = (1 \,..\, Len(stack))$
$\land Len(stack) \in Nat$
⟨3⟩1. $stack \in Seq(\text{SUBSET } Y)$
BY ⟨1⟩3 DEF *TypeInv*
⟨3⟩ QED
BY ⟨3⟩1, *LenProperties*

⟨2⟩7. $end \in Nat$
BY ⟨2⟩6 DEF *end*

⟨2⟩8. $\land stack' \in [1 \,..\, Len(stack') \to \text{SUBSET } Y]$
$\land (\text{DOMAIN } stack') = (1 \,..\, Len(stack'))$
$\land Len(stack') \in Nat$
⟨3⟩1. $stack' \in Seq(\text{SUBSET } Y)$
BY ⟨1⟩3 DEF *TypeInv*
⟨3⟩ QED
BY ⟨3⟩1, *LenProperties*

⟨2⟩9. $\land stack \neq \langle\rangle$
$\land \lor Collect$
$\lor Expand$
BY ⟨1⟩3 DEF *Next*

⟨2⟩10. $\land end \in (Nat \setminus \{0\})$
$\land (end - 1) \in Nat$
⟨4⟩1. $end \in Nat$

BY ⟨2⟩7

⟨4⟩2. $end \neq 0$

⟨5⟩1. $stack \neq \langle\rangle$

BY ⟨2⟩9

⟨5⟩ QED

BY ⟨2⟩6, ⟨5⟩1, *EmptySeq* DEF *end*

⟨4⟩ QED

BY ⟨4⟩1, ⟨4⟩2

This is almost theorem FrontProperties from the module SequenceTheorems, for the case of $end \neq 0$.

⟨2⟩11. LET $sub \triangleq SubSeq(stack, 1, end - 1)$

IN $\land\ sub \in Seq(\text{SUBSET } Y)$

$\land\ Len(sub) = (end - 1)$

$\land\ \forall\, n \in 1 \,..\, (end - 1) :$

$\land\ n \in \text{DOMAIN } sub$

$\land\ sub[n] = stack[n]$

⟨3⟩ DEFINE

$a \triangleq 1$

$b \triangleq end - 1$

$sub \triangleq SubSeq(stack, a, b)$

⟨3⟩1. $stack \in Seq(\text{SUBSET } Y)$

BY ⟨2⟩6

⟨3⟩2. $a \in (1 \,..\, (Len(stack) + 1))$

BY ⟨2⟩10 DEF *end*, *a*

⟨3⟩3. $b \in ((a - 1) \,..\, Len(stack))$

BY ⟨2⟩10 DEF *end*, *a*, *b*

⟨3⟩4. $\land\ sub \in Seq(\text{SUBSET } Y)$

$\land\ Len(sub) = b - a + 1$

BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, *SubSeqProperties* DEF *sub*

⟨3⟩5. $\land\ (\text{DOMAIN } sub) = 1 \,..\, (end - 1)$

$\land\ Len(sub) = (end - 1)$

⟨4⟩1. $(\text{DOMAIN } sub) = 1 \,..\, Len(sub)$

BY ⟨3⟩4, *LenProperties*

⟨4⟩2. $Len(sub) = (end - 1)$

BY ⟨3⟩4, ⟨2⟩10 DEF *a*, *b*

⟨4⟩ QED

BY ⟨4⟩1, ⟨4⟩2, ⟨2⟩10

⟨3⟩7. SUFFICES

ASSUME NEW $n \in 1 \,..\, (end - 1)$

PROVE $\land\ n \in \text{DOMAIN } sub$

$\land\ sub[n] = stack[n]$

BY ⟨3⟩4, ⟨3⟩5, ⟨3⟩7 DEF *sub*, *a*, *b*

⟨3⟩6. $n \in \text{DOMAIN } sub$

BY ⟨3⟩7, ⟨3⟩5 DEF *sub*, *a*, *b*

⟨3⟩8. $sub[n] = stack[n]$
⟨4⟩1. $\forall j \in 1 \,..\, (b - a \quad + 1) :$
$sub[j] = stack[a + j - 1]$
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, *SubSeqProperties* DEF *sub*
⟨4⟩2. $\forall j \in 1 \,..\, (b - a + 1) :$
$sub[j] = stack[j]$
BY ⟨4⟩1, ⟨2⟩10 DEF *a*
⟨4⟩3. DOMAIN $sub = 1 \,..\, (b - a + 1)$
BY ⟨3⟩4, *LenProperties*
⟨4⟩ QED
BY ⟨3⟩6, ⟨4⟩2, ⟨4⟩3
⟨3⟩ QED
BY ⟨3⟩6, ⟨3⟩8
⟨2⟩12. PICK $q \in$ DOMAIN $stack : IsPrefixCov(stack[q], g)$
BY ⟨2⟩3, ⟨2⟩5
⟨2⟩13. $q \in 1 \,..\, Len(stack)$
⟨3⟩1. $q \in$ DOMAIN $stack$
BY ⟨2⟩12
⟨3⟩ QED
BY ⟨3⟩1, ⟨2⟩6

If the partial cover that is a prefix of C is not in the last element on the stack, then it remains where it is in stack .

⟨2⟩14. ASSUME $q < Len(stack)$
PROVE $\exists\, n \in$ DOMAIN $stack' : IsPrefixCov(stack[n]', g)$

⟨3⟩1. $q \in 1 \,..\, (end - 1)$
⟨4⟩1. $q \in 1 \,..\, end$
BY ⟨2⟩13 DEF *end*
⟨4⟩2. $q < end$
BY ⟨2⟩14 DEF *end*
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2, ⟨2⟩7

⟨3⟩2. $\wedge\, stack[q]' = stack[q]$
$\wedge\, q \in$ DOMAIN $stack'$
⟨4⟩1.CASE *Collect*
⟨5⟩1. $stack' = SubSeq(stack, 1, end - 1)$
BY ⟨4⟩1 DEF *Collect*, *end*
⟨5⟩ QED
BY ⟨5⟩1, ⟨3⟩1, ⟨2⟩11
⟨4⟩2.CASE *Expand*
⟨5⟩1. $stack' = front \circ more$
BY ⟨4⟩2 DEF *Expand*, *front*, *more*, *enum*, *succ*, *ymax*, *Q*, *k*, *i*, *PartialCover*, *end*
⟨5⟩2. $\wedge\, stack[q]' = front[q]$

$\land\ q \in$ DOMAIN $stack'$

⟨6⟩1. $\land\ front \in Seq($SUBSET $Y)$
$\land\ Len(front) = (end - 1)$
BY ⟨2⟩11 DEF $front$

⟨6⟩2. $more \in Seq($SUBSET $Y)$
BY ⟨1⟩3, ⟨2⟩9, $MoreInSeqSubsetY$ DEF end, $PartialCover$, i, k, $ymax$, Q, $succ$, $enum$, $more$

⟨6⟩3. $q \in 1 \,..\, (Len(front) + Len(more))$
⟨7⟩1. $Len(more) \in Nat$
BY ⟨6⟩2, $LenProperties$
⟨7⟩2. $Len(front) = (end - 1)$
BY ⟨6⟩1
⟨7⟩ QED
BY ⟨7⟩1, ⟨7⟩2, ⟨2⟩10, ⟨3⟩1

⟨6⟩4. $q \leq Len(front)$
⟨7⟩1. $Len(front) \in Nat$
BY ⟨6⟩1, $LenProperties$
⟨7⟩ QED
BY ⟨7⟩1, ⟨3⟩1, ⟨2⟩10, ⟨6⟩1

⟨6⟩5. $\land\ stack' \in Seq($SUBSET $Y)$
$\land\ stack[q]' = front[q]$
$\land\ Len(stack') = Len(front) + Len(more)$
BY ⟨6⟩1, ⟨6⟩2, ⟨6⟩3, ⟨6⟩4, ⟨5⟩1, $ConcatProperties$

⟨6⟩6. DOMAIN $stack' = 1 \,..\, (Len(front) + Len(more))$
BY ⟨6⟩5, $LenProperties$

⟨6⟩7. $q \in$ DOMAIN $stack'$
BY ⟨6⟩3, ⟨6⟩6

⟨6⟩ QED
BY ⟨6⟩5, ⟨6⟩7

⟨5⟩3. $front[q] = stack[q]$
BY ⟨3⟩1, ⟨2⟩11 DEF $front$

⟨5⟩ QED
BY ⟨5⟩2, ⟨5⟩3

⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2, ⟨2⟩9
⟨4⟩1, ⟨4⟩2 are exhaustive by ⟨2⟩9

⟨3⟩3. $IsPrefixCov(stack[q]', g)$
⟨4⟩1. $IsPrefixCov(stack[q], g)$
BY ⟨2⟩12

⟨4⟩2. $stack[q] = stack[q]'$
BY ⟨3⟩2

⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2

⟨3⟩ QED

BY $\langle 3\rangle 2$, $\langle 3\rangle 3$

So it suffices to consider only the case of q as last element.

$\langle 2\rangle 15$. SUFFICES
ASSUME
$q = Len(stack)$
PROVE
$\lor \exists\, n \in \text{DOMAIN } stack' : \ IsPrefixCov(stack[n]', g)$
$\lor \ C \in MinCoversBelow'$

$\langle 3\rangle$ QED goal from $\langle 2\rangle 5$
BY $\langle 2\rangle 13$, $\langle 2\rangle 14$, $\langle 2\rangle 15$, $\langle 2\rangle 7$ DEF *end*

$\langle 2\rangle 16$. $PartialCover = stack[q]$
$\langle 3\rangle 1$. $q = end$
BY $\langle 2\rangle 15$ DEF *end*
$\langle 3\rangle$ QED
BY $\langle 3\rangle 1$ DEF *PartialCover*

$\langle 2\rangle 17$. $\land\ i \in 0 \,..\, N$
$\land\ PartialCover \in \text{SUBSET } Y$

$\langle 3\rangle 1$. $stack \in Seq(\text{SUBSET } Y)$
BY $\langle 1\rangle 3$ DEF *TypeInv*
$\langle 3\rangle 2$. $\land\ Len(stack) \in Nat$
$\land\ (\text{DOMAIN } stack) = 1 \,..\, Len(stack)$
$\land\ stack \in [1 \,..\, Len(stack) \to \text{SUBSET } Y]$
BY $\langle 3\rangle 1$, *LenProperties*
$\langle 3\rangle 3$. $q \in \text{DOMAIN } stack$
BY $\langle 2\rangle 15$, $\langle 3\rangle 2$
$\langle 3\rangle 4$. $stack[q] \in \text{SUBSET } Y$
BY $\langle 3\rangle 2$, $\langle 3\rangle 3$
$\langle 3\rangle 5$. $PartialCover \in \text{SUBSET } Y$
BY $\langle 2\rangle 16$, $\langle 3\rangle 4$
$\langle 3\rangle 6$. $IsFiniteSet(Y)$
BY *XYAreFiniteSets*
$\langle 3\rangle 7$. $IsFiniteSet(PartialCover)$
BY $\langle 3\rangle 5$, $\langle 3\rangle 6$, *FS_Subset*
$\langle 3\rangle 8$. $Cardinality(PartialCover) \in Nat$
BY $\langle 3\rangle 7$, *FS_CardinalityType*
$\langle 3\rangle 9$. $i \in Nat$
BY $\langle 3\rangle 8$ DEF i
$\langle 3\rangle 10$. $(i < N) \lor (i = N)$
BY $\langle 1\rangle 3$ DEF *Next*, *Collect*, *Expand*, i, *PartialCover*, *end*
$\langle 3\rangle 11$. $i \in 0 \,..\, N$
BY $\langle 3\rangle 9$, $\langle 3\rangle 10$, $\langle 2\rangle 1$
$\langle 3\rangle$ QED
BY $\langle 3\rangle 11$, $\langle 3\rangle 5$

⟨2⟩18. $PartialCover = \{g[t] : \ t \in 1 \,..\, i\}$
⟨3⟩1. $IsPrefixCov(stack[q],\ g)$
BY ⟨2⟩12
⟨3⟩2. $PartialCover = stack[q]$
BY ⟨2⟩16
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2 DEF $IsPrefixCov,\ i,\ PartialCover$
⟨2⟩ USE ⟨2⟩1 $N \in Nat$

The below step asserts that Leq establishes a unique bijection between C and Cm.

⟨2⟩19. $\land\ g \in Bijection(1 \,..\, N,\ C)$
$\land\ \forall\, q1 \in 1 \,..\, N :$
$\land\ Leq[g[q1],\ Lm[q1]]$
$\land\ \forall\, p \in 1 \,..\, N \setminus \{q1\} :$
$\land\ \neg Leq[g[p],\ Lm[q1]]$
$\land\ \neg Leq[g[q1],\ Lm[p]]$

⟨3⟩1. $IsAMinCover(C,\ X,\ Y,\ Leq)$
BY ⟨2⟩2
⟨3⟩2. $IsAMinCover(Cm,\ X,\ Y,\ Leq)$
⟨4⟩1. $IsAMinCover(Cm,\ X,\ Max,\ Leq)$
OBVIOUS
⟨4⟩ QED
BY ⟨4⟩1, $MinCoverFromMaxYIsMinCoverFromY$ DEF Max
⟨3⟩3. $Refines(C,\ Cm,\ Leq)$
⟨4⟩1. $C \in AllCandidatesBelow(Cm,\ Y)$
OBVIOUS
⟨4⟩ QED
BY ⟨4⟩1 DEF $AllCandidatesBelow$ $S \leftarrow C$
⟨3⟩ QED
BY $MinCoverRefinementInducesBijection$,
⟨3⟩1, ⟨3⟩2, ⟨3⟩3 DEF g

⟨2⟩20. $C = \{g[t] : \ t \in 1 \,..\, N\}$
BY ⟨2⟩19 DEF $Bijection,\ Surjection$
⟨2⟩21. ASSUME $i = N$
PROVE $C \in MinCoversBelow'$

⟨3⟩1. $Collect$
⟨4⟩1. $\land\ stack \neq \langle\rangle$
$\land\ \lor\ Collect$
$\lor\ Expand$
BY ⟨1⟩3 DEF $Next$
⟨4⟩2. $\neg Expand$
⟨5⟩1. $\neg(i < N)$

BY $\langle 2\rangle 21$, $\langle 2\rangle 17$

$\langle 5\rangle$ QED
BY $\langle 5\rangle 1$ DEF *Expand*, *i*, *PartialCover*, *end*

$\langle 4\rangle$ QED
BY $\langle 4\rangle 1$, $\langle 4\rangle 2$

$\langle 3\rangle 2$. $PartialCover = C$

$\langle 4\rangle 1$. $PartialCover = \{g[t] : \ t \in 1 \,..\, N\}$
BY $\langle 2\rangle 18$, $\langle 2\rangle 21$

$\langle 4\rangle$ QED
BY $\langle 4\rangle 1$, $\langle 2\rangle 20$

$\langle 3\rangle 3$. $PartialCover \in MinCoversBelow'$

$\langle 4\rangle 1$. $MinCoversBelow' = MinCoversBelow \cup \{PartialCover\}$
BY $\langle 3\rangle 1$ DEF *Collect*, *PartialCover*, *end*

$\langle 4\rangle$ QED
BY $\langle 4\rangle 1$

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

$\langle 2\rangle 22$. SUFFICES
ASSUME $i < N$
PROVE $\exists\, n \in$ DOMAIN $stack' : \ IsPrefixCov(stack[n]', g)$

$\langle 3\rangle 1$. $i \in 0 \,..\, N$
BY $\langle 2\rangle 17$

$\langle 3\rangle 2$. $(i < N) \vee (i = N)$
BY $\langle 3\rangle 1$

$\langle 3\rangle$ QED goal from $\langle 2\rangle 15$
BY $\langle 2\rangle 21$, $\langle 2\rangle 22$, $\langle 3\rangle 2$
$\langle 2\rangle 21$, $\langle 2\rangle 22$ are exhaustive by $\langle 3\rangle 2$

$\langle 2\rangle 23$. $k \in 1 \,..\, N$

$\langle 3\rangle 1$. $N \in Nat$
BY $\langle 2\rangle 1$

$\langle 3\rangle 2$. $i \in 0 \,..\, (N - 1)$
BY $\langle 2\rangle 17$, $\langle 2\rangle 22$

$\langle 3\rangle 3$. $k = i + 1$
BY DEF k

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

$\langle 2\rangle 24$. $\wedge\, y \ \in C$
$\wedge\, y \ \in Y$

$\langle 3\rangle 1$. $y \in C$

$\langle 4\rangle 1$. $k \in 1 \,..\, N$
BY $\langle 2\rangle 22$, $\langle 2\rangle 17$ DEF k

⟨4⟩ QED
BY ⟨2⟩19, ⟨4⟩1 DEF y, *Bijection*, *Surjection*
⟨3⟩2. $C \subseteq Y$
BY ⟨2⟩2 DEF *IsAMinCover*
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2

⟨2⟩25. ASSUME $y \notin succ$
PROVE FALSE C cannot be a cover in this case.
⟨3⟩1. $k \in 1 \,..\, N$
⟨4⟩1. $i \in 0 \,..\, (N-1)$
BY ⟨2⟩17, ⟨2⟩22
⟨4⟩2. $k = i + 1$
BY DEF k
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2, ⟨2⟩1
⟨3⟩2. PICK $x \in Only(ymax,\ Q) :\ \neg Leq[x,\ y]$
⟨4⟩1. $y \in Y$
BY ⟨2⟩24
⟨4⟩2. $Leq[y,\ ymax]$
⟨5⟩1. $k = i + 1$
BY DEF k
⟨5⟩2. $i \in 0 \,..\, (N-1)$
BY ⟨2⟩17, ⟨2⟩22
⟨5⟩3. $k \in 1 \,..\, N$
BY ⟨5⟩1, ⟨5⟩2, ⟨2⟩1
⟨5⟩4. $Leq[g[k],\ Lm[k]]$
BY ⟨2⟩19, ⟨5⟩3
⟨5⟩ QED
BY ⟨5⟩4 DEF y, $ymax$
⟨4⟩3. $y \notin \{$
$y1 \in Y :\ \wedge\ Leq[y1,\ ymax]$
$\wedge\ \forall\, q1 \in Only(ymax,\ Q) :\ Leq[q1,\ y1]\}$
BY ⟨2⟩25 DEF *succ*, *BelowAndSuff*
⟨4⟩4. $\neg \forall\, q1 \in Only(ymax,\ Q) :\ Leq[q1,\ y]$
BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3
⟨4⟩5. $\exists\, q1 \in Only(ymax,\ Q) :\ \neg Leq[q1,\ y]$
BY ⟨4⟩4
⟨4⟩ QED
BY ⟨4⟩5
⟨3⟩3. PICK $yc \in C :\ Leq[x,\ yc]$
⟨4⟩1. ASSUME NEW $u \in X$
PROVE $\exists\, yc \in C :\ Leq[u,\ yc]$
⟨5⟩1. $IsAMinCover(C,\ X,\ Y,\ Leq)$
BY ⟨2⟩2

⟨5⟩2. $IsACover(C,\ X,\ Leq)$
BY ⟨5⟩1, *MinCoverProperties*
⟨5⟩ QED
BY ⟨5⟩2 DEF *IsACover*
⟨4⟩2. $x \in X$
BY ⟨3⟩2 DEF *Only*
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2
⟨3⟩4. $yc \neq y$
⟨4⟩1. SUFFICES
ASSUME $yc = y$
PROVE FALSE
BY ⟨4⟩1
⟨4⟩2. $\neg Leq[x,\ y]$
BY ⟨3⟩2
⟨4⟩3. $Leq[x,\ y]$
⟨5⟩1. $Leq[x,\ yc]$
BY ⟨3⟩3
⟨5⟩ QED
BY ⟨5⟩1, ⟨4⟩1
⟨4⟩ QED goal from ⟨4⟩1
BY ⟨4⟩2, ⟨4⟩3
⟨3⟩5. ASSUME $yc \in PartialCover$
PROVE FALSE
⟨4⟩1. $yc \in Q \setminus \{ymax\}$
⟨5⟩1. $yc \in Q$
BY ⟨3⟩5 DEF Q
⟨5⟩2. $yc \neq ymax$
⟨6⟩1. SUFFICES ASSUME $yc = ymax$
PROVE FALSE
BY ⟨6⟩1
⟨6⟩2. $Leq[yc,\ ymax]$
⟨7⟩1. $yc \in C$
BY ⟨3⟩3
⟨7⟩2. $C \in$ SUBSET Y
OBVIOUS
⟨7⟩3. $yc \in Z$
BY ⟨7⟩1, ⟨7⟩2, *ProblemInput*
⟨7⟩ QED
BY ⟨6⟩1, ⟨7⟩3, *LeqIsPor*
DEF *IsAPartialOrder*, *IsReflexive*, Z
⟨6⟩3. $i \in 0 \,..\, (N-1)$
BY ⟨2⟩17, ⟨2⟩22
⟨6⟩4. PICK $t \in 1 \,..\, i :\ yc = g[t]$
⟨7⟩1. $PartialCover = \{g[t] :\ t \in 1 \,..\, i\}$

BY ⟨2⟩18
⟨7⟩ QED
BY ⟨3⟩5, ⟨7⟩1
⟨6⟩5. $k \in 1 \,..\, N \setminus \{t\}$
⟨7⟩ USE ⟨2⟩1 $N \in Nat$
⟨7⟩1. $k = i + 1$
BY DEF k
⟨7⟩3. $k \in (i+1) \,..\, N$
BY ⟨7⟩1, ⟨6⟩3
⟨7⟩4. $t \in 1 \,..\, i$
BY ⟨6⟩4
⟨7⟩5. $k \neq t$
BY ⟨6⟩3, ⟨7⟩3, ⟨7⟩4
⟨7⟩ QED
BY ⟨7⟩5, ⟨3⟩1
⟨6⟩6. $\neg Leq[g[t],\ Lm[k]]$
⟨7⟩1. $t \in 1 \,..\, N$
BY ⟨6⟩4, ⟨6⟩3
⟨7⟩ QED
BY ⟨2⟩19, ⟨7⟩1, ⟨6⟩5 $q \leftarrow t,\ p \leftarrow k$
⟨6⟩7. $\neg Leq[yc,\ ymax]$
⟨7⟩1. $yc = g[t]$
BY ⟨6⟩4
⟨7⟩2. $ymax = Lm[k]$
BY DEF $ymax$
⟨7⟩ QED
BY ⟨6⟩6, ⟨7⟩1, ⟨7⟩2
⟨6⟩ QED goal from ⟨6⟩1
BY ⟨6⟩2, ⟨6⟩7
⟨5⟩ QED
BY ⟨5⟩1, ⟨5⟩2
⟨4⟩2. $\forall\, yother \in Q \setminus \{ymax\} :\ \neg Leq[x,\ yother]$
BY ⟨3⟩2 DEF $Only$
⟨4⟩3. $\neg Leq[x,\ yc]$
BY ⟨4⟩1, ⟨4⟩2
⟨4⟩ QED
BY ⟨3⟩3, ⟨4⟩3
⟨3⟩6. ASSUME $yc \in After$
PROVE FALSE
⟨4⟩1. PICK $t \in (k+1) \,..\, N :\ yc = g[t]$
⟨5⟩1. $After = \{g[t] :\ t \in (k+1) \,..\, N\}$
BY DEF $After$
⟨5⟩2. $yc \in \{g[t] :\ t \in (k+1) \,..\, N\}$
BY ⟨3⟩6, ⟨5⟩1
⟨5⟩ QED

BY ⟨5⟩2
⟨4⟩2. DEFINE $yt \triangleq Lm[t]$
⟨4⟩3. $t \in 1 \,..\, N$
⟨5⟩1. $t \in (k+1) \,..\, N$
BY ⟨4⟩1
⟨5⟩2. $k \in 1 \,..\, N$
BY ⟨3⟩1
⟨5⟩ QED
BY ⟨5⟩1, ⟨5⟩2
⟨4⟩4. $Leq[yc,\ yt]$
⟨5⟩2. $Leq[g[t],\ Lm[t]]$
BY ⟨2⟩19, ⟨4⟩3
⟨5⟩3. $yc = g[t]$
BY ⟨4⟩1
⟨5⟩4. $yt = Lm[t]$
BY DEF yt
⟨5⟩ QED
BY ⟨5⟩2, ⟨5⟩3, ⟨5⟩4
⟨4⟩5. $Leq[x,\ yt]$
⟨5⟩1. $Leq[x,\ yc]$
BY ⟨3⟩3
⟨5⟩2. $Leq[yc,\ yt]$
BY ⟨4⟩4
⟨5⟩3. $IsTransitive(Leq)$
BY *ProblemInput* DEF *IsACompleteLattice*, *IsAPartialOrder*
⟨5⟩4. $\land\ x \in Z$
$\land\ yc \in Z$
$\land\ yt \in Z$
⟨6⟩1. $x \in Z$
⟨7⟩1. $x \in X$
BY ⟨3⟩2 DEF *Only*
⟨7⟩2. $X \subseteq Z$
BY *ProblemInput*
⟨7⟩ QED
BY ⟨7⟩1, ⟨7⟩2
⟨6⟩2. $yc \in Z$
⟨7⟩1. $yc \in C$
BY ⟨3⟩3
⟨7⟩2. $C \subseteq Y$
BY ⟨2⟩2 DEF *IsAMinCover*
⟨7⟩3. $Y \subseteq Z$
BY *ProblemInput*
⟨7⟩ QED
BY ⟨7⟩1, ⟨7⟩2, ⟨7⟩3

⟨6⟩3. $yt \in Z$
⟨7⟩1. $Lm[t] \in Cm$
⟨8⟩1. $t \in 1 \,..\, N$
BY ⟨4⟩3
⟨8⟩ QED
BY ⟨8⟩1, ⟨1⟩2, *LmIsBijection* DEF *Bijection*, *Injection*
⟨7⟩2. $Cm \subseteq Y$
BY ⟨1⟩2
⟨7⟩3. $Y \subseteq Z$
BY *ProblemInput*
⟨7⟩ QED
BY ⟨7⟩1, ⟨7⟩2, ⟨7⟩3 DEF *yt*
⟨6⟩ QED
BY ⟨6⟩1, ⟨6⟩2, ⟨6⟩3
⟨5⟩ QED
BY ⟨5⟩1, ⟨5⟩2, ⟨5⟩3, ⟨5⟩4 DEF *IsTransitive*, *Z*
⟨4⟩6. $yt \in Q \setminus \{ymax\}$
⟨5⟩1. $yt \in Q$
⟨6⟩1. $yt \in Patch(k)$
⟨7⟩1. $t \in (k+1) \,..\, N$
BY ⟨4⟩1
⟨7⟩2. $Patch(k) = Image(Lm,\, k \,..\, N)$
BY DEF *Patch*
⟨7⟩3. $Patch(k) = \{Lm[j] : \; j \in k \,..\, N\}$
BY ⟨7⟩2 DEF *Image*
⟨7⟩4. $t \in k \,..\, N$
BY ⟨7⟩1, ⟨3⟩1
⟨7⟩5. $Lm[t] \in Patch(k)$
BY ⟨7⟩3, ⟨7⟩4
⟨7⟩ QED
BY ⟨7⟩5 DEF *yt*
⟨6⟩ QED
BY ⟨6⟩1 DEF *Q*
⟨5⟩2. $yt \neq ymax$
⟨6⟩ USE ⟨2⟩1 $N \in Nat$
⟨6⟩1. $Lm \in Injection(1 \,..\, N,\, Cm)$
BY ⟨1⟩2, *LmIsBijection* DEF *Bijection*
⟨6⟩2. $t \in (k+1) \,..\, N$
BY ⟨4⟩1
⟨6⟩3. $k \in 1 \,..\, N$
BY ⟨3⟩1
⟨6⟩4. $\wedge\, k \in$ DOMAIN Lm
$\wedge\, t \in$ DOMAIN Lm
⟨7⟩1. $(1 \,..\, N) = (\text{DOMAIN } Lm)$

BY ⟨6⟩1 DEF *Injection*

⟨7⟩2. $k \in$ DOMAIN Lm

BY ⟨7⟩1, ⟨6⟩3

⟨7⟩3. $t \in 1 \,..\, N$

BY ⟨6⟩2, ⟨6⟩3, ⟨2⟩1

⟨7⟩ QED

BY ⟨7⟩1, ⟨7⟩2, ⟨7⟩3

⟨6⟩5. $k \neq t$

BY ⟨6⟩2, ⟨6⟩3

⟨6⟩6. $Lm[k] \neq Lm[t]$

BY ⟨6⟩1, ⟨6⟩4, ⟨6⟩5 DEF *Injection*

⟨6⟩ QED

⟨7⟩1. $ymax = Lm[k]$

BY DEF *ymax*

⟨7⟩2. $yt = Lm[t]$

BY DEF *yt*

⟨7⟩ QED

BY ⟨6⟩6, ⟨7⟩1, ⟨7⟩2

⟨5⟩ QED

BY ⟨5⟩1, ⟨5⟩2

⟨4⟩7. $\forall\, yother \in Q \setminus \{ymax\} :\ \neg Leq[x,\, yother]$

BY ⟨3⟩2 DEF *Only*

⟨4⟩8. $\neg Leq[x,\, yt]$

BY ⟨4⟩6, ⟨4⟩7 $yother \leftarrow yt$

⟨4⟩ QED

BY ⟨4⟩5, ⟨4⟩8

⟨3⟩7. $yc \notin (PartialCover \cup \{y\} \cup After)$

BY ⟨3⟩4, ⟨3⟩5, ⟨3⟩6

⟨3⟩8. $C = (PartialCover \cup \{y\} \cup After)$

⟨4⟩1. $PartialCover = \{g[t] :\ t \in 1 \,..\, i\}$

BY ⟨2⟩18

⟨4⟩2. $i \in 0 \,..\, (N-1)$

BY ⟨2⟩17, ⟨2⟩22

⟨4⟩3. $k = i + 1$

BY DEF *k*

⟨4⟩4. $k \in 1 \,..\, N$

BY ⟨4⟩2, ⟨4⟩3, ⟨2⟩1

⟨4⟩5. $After = \{g[t] :\ t \in (k+1) \,..\, N\}$

BY DEF *After*

⟨4⟩6. $PartialCover = \{g[t] :\ t \in 1 \,..\, (k-1)\}$

BY ⟨4⟩1, ⟨4⟩3, ⟨4⟩2

⟨4⟩7. $y = g[k]$

BY DEF *y*

⟨4⟩8. $(1 \,..\, N) = ((1 \,..\, (k-1)) \cup \{k\} \cup ((k+1) \,..\, N))$

BY ⟨4⟩4, ⟨2⟩1

⟨4⟩9. $\{g[t] : \ t \in 1 \,..\, N\} = (PartialCover \cup \{y\} \cup After)$
BY ⟨4⟩5, ⟨4⟩6, ⟨4⟩7, ⟨4⟩8
⟨4⟩10. $C = \{g[t] : \ t \in 1 \,..\, N\}$
BY ⟨2⟩20
⟨4⟩ QED
BY ⟨4⟩9, ⟨4⟩10
⟨3⟩9. $yc \notin C$
BY ⟨3⟩7, ⟨3⟩8
⟨3⟩ QED
BY ⟨3⟩3, ⟨3⟩9

⟨2⟩26. ASSUME $y \in succ$
PROVE $\exists\, n \in$ DOMAIN $stack' : \ IsPrefixCov(stack[n]', g)$
⟨3⟩ DEFINE
$Ns \triangleq Cardinality(succ)$
⟨3⟩1. $enum \in Bijection(1 \,..\, Ns, succ)$
⟨4⟩1. $enum =$ CHOOSE $f : \ f \in Bijection(1 \,..\, Ns, succ)$
BY DEF $enum$, $Enumerate$, Ns
⟨4⟩2. $Bijection(1 \,..\, Ns, succ) \neq \{\}$
⟨5⟩1. PICK $n \in Nat : \ ExistsBijection(1 \,..\, n, succ)$
⟨6⟩1. $IsFiniteSet(succ)$
⟨7⟩1. $BelowAndSuff(ymax, Q, Y) \subseteq Y$
BY DEF $BelowAndSuff$
⟨7⟩2. $succ \subseteq Y$
BY ⟨7⟩1 DEF $succ$
⟨7⟩3. $IsFiniteSet(Y)$
BY $XYAreFiniteSets$
⟨7⟩ QED
BY ⟨7⟩2, ⟨7⟩3, FS_Subset
⟨6⟩ QED
BY ⟨6⟩1, $FS\_NatBijection$
⟨5⟩2. $n = Cardinality(succ)$
BY ⟨5⟩1, $FS\_CountingElements$
⟨5⟩3. $ExistsBijection(1 \,..\, Ns, succ)$
BY ⟨5⟩1, ⟨5⟩2 DEF Ns
⟨5⟩ QED
BY ⟨5⟩3 DEF $ExistsBijection$
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2
⟨3⟩2. PICK $r \in$ DOMAIN $enum : \ enum[r] = y$
⟨4⟩1. $y \in succ$
BY ⟨2⟩26
⟨4⟩2. $\exists\, r \in (1 \,..\, Ns) : \ enum[r] = y$
BY ⟨3⟩1, ⟨4⟩1 DEF $Bijection$, $Surjection$
⟨4⟩3. (DOMAIN $enum$) $= (1 \,..\, Ns)$

BY $\langle 3\rangle 1$ DEF *Bijection*, *Surjection*

$\langle 4\rangle$ QED

BY $\langle 4\rangle 2$, $\langle 4\rangle 3$

$\langle 3\rangle 3$. $\land\ r \in$ DOMAIN *more*

$\land\ r \in Nat$

$\langle 4\rangle 1$. $\land$ (DOMAIN *enum*) $= (1\ ..\ Len(enum))$

$\land\ Len(enum) \in Nat$

$\langle 5\rangle 1$. $enum \in [1\ ..\ Ns \to succ]$

BY $\langle 3\rangle 1$ DEF *Bijection*, *Surjection*

$\langle 5\rangle 2$. $Ns \in Nat$

$\langle 6\rangle 1$. $IsFiniteSet(succ)$

BY *BelowAndSuffIsFinite*, *XYAreFiniteSets* DEF *succ*

$\langle 6\rangle$ QED

BY $\langle 6\rangle 1$, *FS_CardinalityType*

$\langle 5\rangle 3$. $enum \in Seq(succ)$

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$ DEF *Seq*

$\langle 5\rangle$ QED

BY $\langle 5\rangle 3$, *LenProperties*

$\langle 4\rangle 2$. (DOMAIN *more*) $= (1\ ..\ Len(enum))$

BY DEF *more*

$\langle 4\rangle 3$. $\land$ (DOMAIN *enum*) $=$ (DOMAIN *more*)

$\land$ (DOMAIN *enum*) $\subseteq Nat$

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$

$\langle 4\rangle$ QED

BY $\langle 3\rangle 2$, $\langle 4\rangle 3$

$\langle 3\rangle 4$. $more[r] = PartialCover \cup \{enum[r]\}$

BY $\langle 3\rangle 3$ DEF *more*

$\langle 3\rangle$ DEFINE

$W \triangleq PartialCover \cup \{enum[r]\}$

$\langle 3\rangle$ HIDE DEF W

$\langle 3\rangle 5$. $\land\ W = \{g[t] :\ t \in 1\ ..\ (i+1)\}$

$\land\ y\ \in W$

$\langle 4\rangle 1$. $W = PartialCover \cup \{y\}$

BY $\langle 3\rangle 2$ DEF W

$\langle 4\rangle 2$. $PartialCover = \{g[t] :\ t \in 1\ ..\ i\}$

BY $\langle 2\rangle 18$

$\langle 4\rangle 3$. $y = g[i+1]$

$\langle 5\rangle 1$. $y = g[k]$

BY DEF y

$\langle 5\rangle 2$. $k = i+1$

BY DEF k

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle 4$. $W = \{g[t] :\ t \in 1\ ..\ i\} \cup \{g[i+1]\}$

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$

⟨4⟩5. $(i \in 0 \,..\, N) \land (N \in Nat)$
BY ⟨2⟩17, ⟨2⟩1
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩4, ⟨4⟩5
⟨3⟩6. $Cardinality(W) = k$
⟨4⟩1. $g \in Bijection(1 \,..\, N,\ C)$
BY ⟨2⟩19
⟨4⟩ DEFINE $gW \triangleq Restrict(g, 1 \,..\, k)$
⟨4⟩2. $gW \in Bijection(1 \,..\, k,\ W)$
⟨5⟩1. $1 \,..\, k \subseteq 1 \,..\, N$
BY ⟨2⟩23, ⟨2⟩1
⟨5⟩2. $gW \in Bijection(1 \,..\, k,\ Range(gW))$
BY ⟨4⟩1, ⟨5⟩1, *Fun_BijRestrict* DEF gW
⟨5⟩3. $Range(gW) = W$
BY ⟨3⟩5 DEF W, $Range$, gW, $Restrict$, k
⟨5⟩ QED
BY ⟨5⟩2, ⟨5⟩3
⟨4⟩ QED
BY ⟨2⟩23, ⟨4⟩2, *FS_CountingElements* DEF *ExistsBijection*
⟨3⟩7. $stack' = front \circ more$
⟨4⟩1. $\lor\ Collect$
$\lor\ Expand$
BY ⟨1⟩3 DEF *Next*
⟨4⟩2. $i \in 0 \,..\, (N - 1)$
⟨5⟩1. $i \in 0 \,..\, N$
BY ⟨2⟩17
⟨5⟩2. $N \in Nat$
BY ⟨2⟩1
⟨5⟩3. $i < N$
BY ⟨2⟩22
⟨5⟩ QED
BY ⟨5⟩1, ⟨5⟩2, ⟨5⟩3
⟨4⟩3. $\neg(i = N)$
BY ⟨4⟩2, ⟨2⟩1
⟨4⟩4. $\neg Collect$
BY ⟨4⟩3 DEF $Collect$, i, $PartialCover$, end
⟨4⟩5. $Expand$
BY ⟨4⟩1, ⟨4⟩4
⟨4⟩ QED
BY ⟨4⟩5 DEF $Expand$, $front$, $more$, end,
$enum$, $succ$, Q, $ymax$, k, i, $PartialCover$
⟨3⟩8. PICK $n \in$ DOMAIN $stack' : stack[n]' = more[r]$
⟨4⟩ DEFINE
$fm \triangleq Len(front) + Len(more)$
$j \triangleq r + Len(front)$

⟨4⟩ HIDE DEF fm, j
⟨4⟩1. $stack' = front \circ more$
BY ⟨3⟩7
⟨4⟩2. $\land\ r \in$ DOMAIN $more$
$\land\ r \in Nat$
BY ⟨3⟩3
⟨4⟩3. $more \in Seq(\text{SUBSET}\ Y)$
BY ⟨1⟩3, $MoreInSeqSubsetY$ DEF $Next$, end, $PartialCover$, i, k, $ymax$, Q, $succ$, $enum$, $more$
⟨4⟩4. $front \in Seq(\text{SUBSET}\ Y)$
BY ⟨2⟩11 DEF $front$
⟨4⟩5. $\land\ Len(more) \in Nat$
$\land\ Len(front) \in Nat$
BY ⟨4⟩3, ⟨4⟩4, $LenProperties$
⟨4⟩6. $\land$ DOMAIN $stack' = 1 \,..\, fm$
$\land \forall\, d \in 1 \,..\, fm :$
$\lor \neg(d > Len(front))$
$\lor\ stack[d]' = more[d - Len(front)]$
BY ⟨4⟩1, ⟨4⟩3, ⟨4⟩4, $ConcatProperties$, $LenProperties$ DEF fm
⟨4⟩7. $\land\ j \in 1 \,..\, fm$
$\land\ j > Len(front)$
⟨5⟩1. $r \in 1 \,..\, Len(more)$
BY ⟨4⟩2, ⟨4⟩3, $LenProperties$
⟨5⟩ QED
BY ⟨5⟩1, ⟨4⟩5 DEF j, fm
⟨4⟩8. $\exists\, n \in 1 \,..\, fm :$
$\land\ n = j$
$\land\ stack[n]' = more[n - Len(front)]$
BY ⟨4⟩6, ⟨4⟩7

Tricky point: cannot use j *in place of* n *here, because the operator* j *is defined as an expression that contains a variable.So it does not necessarily hold that* $stack[j] = more[j - Len(front)]$*, due to the priming operator.*

⟨4⟩9. $(j - Len(front)) = r$
BY ⟨4⟩5, ⟨4⟩2 DEF j
⟨4⟩10. $j \in$ DOMAIN $stack'$
BY ⟨4⟩6, ⟨4⟩7
⟨4⟩ QED
BY ⟨4⟩8, ⟨4⟩9, ⟨4⟩10
⟨3⟩9. $IsPrefixCov(stack[n]',\ g)$
⟨4⟩1. $stack[n]' = more[r]$
BY ⟨3⟩8
⟨4⟩2. $more[r] = PartialCover \cup \{enum[r]\}$

BY $\langle 3\rangle 4$

$\langle 4\rangle 3.\ stack[n]' = W$

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF W

$\langle 4\rangle 4.\ stack[n]' = \{g[t] :\ t \in 1\,..\,k\}$

BY $\langle 4\rangle 3$, $\langle 3\rangle 5$ DEF k

$\langle 4\rangle 5.\ Cardinality(stack[n]') = k$

BY $\langle 4\rangle 3$, $\langle 3\rangle 6$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 5$, $\langle 4\rangle 4$ DEF $IsPrefixCov$

$\langle 3\rangle$ QED

BY $\langle 3\rangle 8$, $\langle 3\rangle 9$

$\langle 2\rangle$ QED *goal from* $\langle 2\rangle 22$

BY $\langle 2\rangle 25$, $\langle 2\rangle 26$

$\langle 1\rangle 4.$ ASSUME $InvCompl(C) \land$ UNCHANGED $vars$

PROVE $InvCompl(C)'$

BY $\langle 1\rangle 4$ DEF $InvCompl$, $vars$

$\langle 1\rangle 5.$ ASSUME $[TypeInv \land TypeInv' \land Next]_{vars} \land InvCompl(C)$

PROVE $InvCompl(C)'$

BY $\langle 1\rangle 3$, $\langle 1\rangle 4$, $\langle 1\rangle 5$

$\langle 1\rangle$ DEFINE

$Inv \triangleq InvCompl(C)$

$Nx \triangleq TypeInv \land TypeInv' \land Next$

$\langle 1\rangle 6.$ ASSUME $Inv \land [Nx]_{vars}$

PROVE Inv'

BY $\langle 1\rangle 5$, $\langle 1\rangle 6$ DEF Inv, Nx, $vars$, $InvCompl$

$\langle 1\rangle$ QED

$\langle 2\rangle 1. \lor \neg \land Inv$
$\land \Box[Nx]_{vars}$
$\lor \Box Inv$

BY $\langle 1\rangle 6$, PTL *RuleINV1*

$\langle 2\rangle 2. \lor \neg \land Init$
$\land \Box[TypeInv \land TypeInv' \land Next]_{vars}$
$\lor \Box InvCompl(C)$

BY $\langle 1\rangle 1$, $\langle 2\rangle 1$ DEF Inv, Nx

$\langle 2\rangle 3. \lor \neg \land Init$
$\land \Box TypeInv$
$\land \Box[Next]_{vars}$
$\lor \Box InvCompl(C)$

BY $\langle 2\rangle 2$, PTL *RuleINV2*

$\langle 2\rangle$ QED

BY $\langle 2\rangle 3$, $TypeOK$ DEF $Spec$

The theorem StackContainsPartialCovers proves that PartialCoversInStack is an inductive invariant.That PartialCoversInStack is an inductive invariant is used in the theorem StrongReductionSoundness to prove that InvSound is an invariant.

THEOREM $StackContainsPartialCovers \triangleq$
  ASSUME
    NEW C,
    $IsAMinCover(Cm, X, Max, Leq)$
  PROVE
    $Spec \Rightarrow \Box PartialCoversInStack$
PROOF
⟨1⟩3. $\wedge\ IsAMinCover(Cm, X, Y, Leq)$
  $\wedge\ Cm \in \text{SUBSET } Y$
  ⟨2⟩1. $IsAMinCover(Cm, X, Max, Leq)$
    OBVIOUS
  ⟨2⟩ QED
    BY ⟨2⟩1, $MinCoverFromMaxYIsMinCoverFromY$,
      $MinCoverProperties$ DEF Max
⟨1⟩4. $N \in Nat$
  BY ⟨1⟩3, $XYAreFiniteSets$, FS_Subset, $FS\_CardinalityType$ DEF N

⟨1⟩1. ASSUME $Init$
  PROVE $PartialCoversInStack$
  ⟨2⟩ DEFINE
    $Partial \triangleq stack[1]$
    $i \triangleq Cardinality(Partial)$
    $k \triangleq i + 1$
    $Q \triangleq Partial \cup Patch(k)$
  ⟨2⟩ HIDE DEF $Partial$, i, k, Q
  ⟨2⟩1. $stack = \langle\{\}\rangle$
    BY ⟨1⟩1 DEF $Init$
  ⟨2⟩5. $Partial = \{\}$
    BY ⟨2⟩1 DEF $Partial$
  ⟨2⟩2. SUFFICES $IsAMinCover(Q, X, Y, Leq)$
    BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩5 DEF Q, k, i, $Partial$, $PartialCoversInStack$
  ⟨2⟩3. $Q = Patch(1)$
    ⟨3⟩2. $k = 1$
      BY ⟨2⟩5, $FS\_EmptySet$ DEF i, k
    ⟨3⟩ QED
      BY ⟨2⟩5, ⟨3⟩2 DEF Q
  ⟨2⟩4. $Q = Cm$
    ⟨3⟩1. $Patch(1) = Image(Lm, 1 \,..\, N)$
      BY ⟨2⟩3 DEF $Patch$
    ⟨3⟩2. $Image(Lm, 1 \,..\, N) = Cm$
      BY ⟨1⟩3, $LmIsBijection$ DEF $Image$, $Bijection$, $Surjection$

⟨3⟩ QED
BY ⟨2⟩3, ⟨3⟩1, ⟨3⟩2
⟨2⟩ QED *goal from ⟨2⟩2*
BY ⟨1⟩3, ⟨2⟩4

⟨1⟩2. ASSUME $TypeInv \land TypeInv' \land Next \land PartialCoversInStack$
PROVE $PartialCoversInStack'$
⟨2⟩1. SUFFICES
ASSUME
NEW $siNext \in$ DOMAIN $stack'$
PROVE
LET
$PartialNext \triangleq stack[siNext]'$
$iNext \triangleq Cardinality(PartialNext)$
$kNext \triangleq iNext + 1$
$QNext \triangleq PartialNext \cup Patch(kNext)$
IN
$\land\ IsAMinCover(QNext,\ X,\ Y,\ Leq)$
$\land\ PartialNext \cap Patch(kNext) = \{\}$
BY ⟨2⟩1 DEF $PartialCoversInStack$

⟨2⟩6. ASSUME
NEW $si \in$ DOMAIN $stack$
PROVE
LET
$Partial \triangleq stack[si]$
$i \triangleq Cardinality(Partial)$
$k \triangleq i + 1$
$Q \triangleq Partial \cup Patch(k)$
IN
$\land\ IsAMinCover(Q,\ X,\ Y,\ Leq)$
$\land\ Partial \cap Patch(k) = \{\}$
⟨3⟩1. $PartialCoversInStack$
BY ⟨1⟩2
⟨3⟩ QED
BY ⟨3⟩1, ⟨2⟩6 DEF $PartialCoversInStack$

⟨2⟩ DEFINE
$end \triangleq Len(stack)$
$front \triangleq SubSeq(stack,\ 1,\ end - 1)$
Definitions pertaining to PartialCoversInStack.
$si \triangleq$ IF $siNext < Len(stack)$ THEN $siNext$ ELSE $Len(stack)$
$Partial \triangleq stack[si]$
$i \triangleq Cardinality(Partial)$
$k \triangleq i + 1$
$Q \triangleq Partial \cup Patch(k)$

Definitions pertaining to Expand.
$PartialE \triangleq stack[end]$
$iE \triangleq Cardinality(PartialE)$
$kE \triangleq iE + 1$
$ymax \triangleq Lm[kE]$
$QE \triangleq PartialE \cup Patch(kE)$
$succ \triangleq BelowAndSuff(ymax,\ QE,\ Y)$
$enum \triangleq Enumerate(succ)$
$more \triangleq [r \in 1\ ..\ Len(enum) \mapsto PartialE \cup \{enum[r]\}]$
Definitions pertaining to PartialCoversInStack .
$PartialNext \triangleq stack[siNext]'$
$iNext \triangleq Cardinality(PartialNext)$
$kNext \triangleq iNext + 1$
$QNext \triangleq PartialNext \cup Patch(kNext)$

$\langle 2\rangle$ HIDE DEF end, si, $Partial$, i, k, Q, $PartialNext$, $iNext$, $kNext$, $QNext$, $PartialE$, $ymax$, QE, iE, kE, $succ$, $enum$, $more$

$\langle 2\rangle 13.\ \wedge stack \in Seq(\text{SUBSET } Y)$
$\wedge stack \in [1\ ..\ Len(stack) \to \text{SUBSET } Y]$
$\wedge (\text{DOMAIN } stack) = (1\ ..\ Len(stack))$
$\wedge Len(stack) \in Nat \setminus \{0\}$ so $end \neq 0$
$\langle 3\rangle 1.\ stack \in Seq(\text{SUBSET } Y)$
BY $\langle 1\rangle 2$ DEF $TypeInv$
$\langle 3\rangle 2.\ stack \neq \langle\rangle$
BY $\langle 1\rangle 2$ DEF $Next$
$\langle 3\rangle$ QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $LenProperties$, $EmptySeq$

$\langle 2\rangle 15.\ \wedge stack' \in Seq(\text{SUBSET } Y)$
$\wedge stack' \in [1\ ..\ Len(stack') \to \text{SUBSET } Y]$
$\wedge Len(stack') \in Nat$
$\langle 3\rangle 1.\ stack' \in Seq(\text{SUBSET } Y)$
BY $\langle 1\rangle 2$ DEF $TypeInv$
$\langle 3\rangle$ QED
BY $\langle 3\rangle 1$, $LenProperties$

$\langle 2\rangle 14.\ \wedge siNext \in 1\ ..\ Len(stack')$
$\wedge siNext \in Nat$
BY $\langle 2\rangle 1$, $\langle 2\rangle 15$

$\langle 2\rangle 16.\ \wedge si \in \text{DOMAIN } stack$
$\wedge si \in 1\ ..\ Len(stack)$

$\langle 3\rangle 1.\ si \in 1\ ..\ Len(stack)$
$\langle 4\rangle 1.$CASE $siNext < Len(stack)$
$\langle 5\rangle 1.\ si = siNext$
BY $\langle 4\rangle 1$ DEF si

⟨5⟩2. ∧ $si \in 1 \,..\, Len(stack')$
∧ $si < Len(stack)$
∧ $Len(stack) \in Nat$
BY ⟨4⟩1, ⟨5⟩1, ⟨2⟩14, ⟨2⟩13
⟨5⟩ QED
BY ⟨5⟩2
⟨4⟩2.CASE $\neg(siNext < Len(stack))$
⟨5⟩1. $si = Len(stack)$
BY ⟨4⟩2 DEF si
⟨5⟩2. $Len(stack) \in Nat \setminus \{0\}$
BY ⟨2⟩13
⟨5⟩ QED
BY ⟨5⟩1, ⟨5⟩2
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2
⟨3⟩2. (DOMAIN $stack$) $= (1 \,..\, Len(stack))$
BY ⟨2⟩13
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2

⟨2⟩12. ∧ $IsAMinCover(Q,\ X,\ Y,\ Leq)$
∧ $Q \in$ SUBSET Y
∧ $IsACover(Q,\ X,\ Leq)$
∧ $IsFiniteSet(Q)$
∧ $Cardinality(Q) = N$
∧ $Cardinality(Q) \in Nat$
⟨3⟩1. $IsAMinCover(Q,\ X,\ Y,\ Leq)$
⟨4⟩1. $PartialCoversInStack$
BY ⟨1⟩2
⟨4⟩2. $si \in$ DOMAIN $stack$
BY ⟨2⟩16
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2, ⟨2⟩6 DEF $PartialCoversInStack$, si, $Partial$, i, k, Q
⟨3⟩2. ∧ $Q \in$ SUBSET Y
∧ $IsACover(Q,\ X,\ Leq)$
BY ⟨3⟩1, $MinCoverProperties$
⟨3⟩3. ∧ $IsFiniteSet(Q)$
∧ $Cardinality(Q) \in Nat$
BY ⟨3⟩2, $XYAreFiniteSets$, FS_Subset, $FS\_CardinalityType$
⟨3⟩4. $Cardinality(Q) = N$
BY ⟨3⟩1, ⟨1⟩3, $AllMinCoversSameCard$, $HaveCardAsCost$, $XYAreFiniteSets$, $ProblemInput$ DEF N
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4

⟨2⟩20. ∧ $front \in Seq(\text{SUBSET } Y)$
∧ $Len(front) = end - 1$
∧ $Len(front) \in Nat$
∧ $\forall j \in 1 \,..\, (end - 1) : \; front[j] = stack[j]$
BY ⟨2⟩13, *FrontProperties*, *LenProperties* DEF *Front*, *front*, *end*

⟨2⟩21. ∧ $more \in Seq(\text{SUBSET } Y)$
∧ $Len(more) \in Nat$
∧ DOMAIN $more = 1 \,..\, Len(more)$
⟨3⟩1. $more \in Seq(\text{SUBSET } Y)$
BY ⟨1⟩2, *MoreInSeqSubsetY* DEF *Next*, *end*, *PartialE*, *iE*, *kE*, *ymax*, *QE*, *succ*, *enum*, *more*
⟨3⟩ QED
BY ⟨3⟩1, *LenProperties*

siNext ∈ *front*
⟨2⟩7. ASSUME $siNext < Len(stack)$
PROVE ∧ $IsAMinCover(QNext, X, Y, Leq)$
∧ $PartialNext \cap Patch(kNext) = \{\}$
⟨3⟩1. $si = siNext$
BY ⟨2⟩7 DEF *si*
⟨3⟩2. $stack[si] = stack[siNext]'$
⟨4⟩5. PICK $r : \; r = si$ *r* has constant level, unlike *si*
OBVIOUS
⟨4⟩1. SUFFICES $stack[r] = stack[r]'$
BY ⟨4⟩1, ⟨3⟩1, ⟨4⟩5
⟨4⟩6. $r \in 1 \,..\, (end - 1)$
BY ⟨4⟩5, ⟨3⟩1, ⟨2⟩7, ⟨2⟩13, ⟨2⟩16 DEF *end*
⟨4⟩2. $Collect \lor Expand$
BY ⟨1⟩2 DEF *Next*
⟨4⟩3.CASE *Collect*
⟨5⟩1. $stack' = front$
BY ⟨4⟩3 DEF *Collect*, *front*, *end*
⟨5⟩ QED
BY ⟨5⟩1, ⟨4⟩6, ⟨2⟩20
⟨4⟩4.CASE *Expand*
⟨5⟩1. $stack[r]' = front[r]$
⟨6⟩1. $stack' = front \circ more$
BY ⟨4⟩4 DEF *Expand*, *front*, *end*, *more*, *enum*, *succ*, *ymax*, *QE*, *kE*, *iE*, *PartialE*
⟨6⟩2. $r \in 1 \,..\, (Len(front) + Len(more))$
⟨7⟩1. $r \in 1 \,..\, Len(front)$
BY ⟨2⟩20, ⟨4⟩6
⟨7⟩2. ASSUME NEW $lf \in Nat$, NEW $lm \in Nat$
PROVE $1 \,..\, lf \subseteq 1 \,..\, (lf + lm)$

BY $\langle 7\rangle 2$

$\langle 7\rangle 3.\ (1\ ..\ Len(front)) \subseteq$
$(1\ ..\ (Len(front) + Len(more)))$
BY $\langle 2\rangle 20$, $\langle 2\rangle 21$, $\langle 7\rangle 2$

$\langle 7\rangle$ QED
BY $\langle 7\rangle 1$, $\langle 7\rangle 3$

$\langle 6\rangle 3.\ r \leq Len(front)$
BY $\langle 4\rangle 6$, $\langle 2\rangle 20$

$\langle 6\rangle$ QED
BY $\langle 2\rangle 20$, $\langle 2\rangle 21$, $\langle 6\rangle 1$, $\langle 6\rangle 2$, $\langle 6\rangle 3$,
ConcatProperties

$\langle 5\rangle 2.\ front[r] = stack[r]$
BY $\langle 4\rangle 6$, $\langle 2\rangle 20$

$\langle 5\rangle$ QED
BY $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle$ QED
BY $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 4$

$\langle 3\rangle 3.\ Q = QNext$
BY $\langle 3\rangle 2$ DEF *Partial*, i, k, Q,
PartialNext, *iNext*, *kNext*, *QNext*

$\langle 3\rangle 4.\ IsAMinCover(QNext,\ X,\ Y,\ Leq)$
BY $\langle 3\rangle 3$, $\langle 2\rangle 12$

$\langle 3\rangle 5.\ PartialNext \cap Patch(kNext) = \{\}$

$\langle 4\rangle 1.\ Partial\ \cap Patch(k) = \{\}$
BY $\langle 2\rangle 6$, $\langle 2\rangle 16$ DEF *Partial*, k, i

$\langle 4\rangle 2.\ PartialNext = Partial$
BY $\langle 3\rangle 2$ DEF *Partial*, *PartialNext*

$\langle 4\rangle 3.\ k = kNext$
BY $\langle 4\rangle 2$ DEF i, k, *iNext*, *kNext*

$\langle 4\rangle$ QED
BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$

$\langle 3\rangle$ QED
BY $\langle 3\rangle 4$, $\langle 3\rangle 5$

siNext $\in$ *more*

$\langle 2\rangle 8.$ SUFFICES
ASSUME $siNext \geq Len(stack)$
PROVE $\land\ IsAMinCover(QNext,\ X,\ Y,\ Leq)$
$\land\ PartialNext \cap Patch(kNext) = \{\}$

$\langle 3\rangle 1.\ siNext \in Nat$
BY $\langle 2\rangle 15$

$\langle 3\rangle 2.\ Len(stack) \in Nat$
BY $\langle 2\rangle 13$

$\langle 3\rangle$ QED goal from $\langle 2\rangle 1$
BY $\langle 2\rangle 7$, $\langle 2\rangle 8$, $\langle 3\rangle 1$, $\langle 3\rangle 2$

DEF $QNext$, $kNext$, $iNext$, $PartialNext$

⟨2⟩18. $si = Len(stack)$
BY ⟨2⟩8, ⟨2⟩13, ⟨2⟩14 DEF si

⟨2⟩17. $i \in Nat$
⟨3⟩1. $stack \in [1 \,..\, Len(stack) \to \text{SUBSET } Y]$
BY ⟨2⟩13
⟨3⟩2. $si \in \text{DOMAIN } stack$
BY ⟨2⟩16
⟨3⟩3. $stack[si] \in \text{SUBSET } Y$
BY ⟨3⟩1, ⟨3⟩2, *ElementOfSeq*
⟨3⟩4. $IsFiniteSet(Y)$
BY *XYAreFiniteSets*
⟨3⟩5. $IsFiniteSet(Partial)$
BY ⟨3⟩3, ⟨3⟩4, *FS_Subset* DEF *Partial*
⟨3⟩ QED
BY ⟨3⟩5, *FS_CardinalityType* DEF i

⟨2⟩19. $\land\ Collect \lor Expand$
$\land\ Partial = stack[end]$
⟨3⟩1. $Collect \lor Expand$
BY ⟨1⟩2 DEF *Next*
⟨3⟩2. $Partial = stack[end]$
BY ⟨2⟩18 DEF *Partial*, *end*
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2

⟨2⟩9. ASSUME $i = N$
PROVE FALSE
⟨3⟩1. *Collect*
⟨4⟩1. $\neg(i < N)$
BY ⟨2⟩9, ⟨2⟩17, ⟨1⟩4
⟨4⟩ QED
BY ⟨4⟩1, ⟨2⟩19 DEF *Expand*, i, *end*
⟨3⟩4. $siNext \geq end$
BY ⟨2⟩8 DEF *end*
⟨3⟩5. $siNext \in 1 \,..\, (end - 1)$
⟨4⟩1. $stack' = SubSeq(stack,\ 1,\ end - 1)$
BY ⟨3⟩1 DEF *Collect*, *end*
⟨4⟩2. $1 \in 1 \,..\, (end + 1)$
BY ⟨2⟩13 DEF *end*
⟨4⟩3. $(end - 1) \in ((1 - 1) \,..\, end)$
BY ⟨2⟩13 DEF *end*
⟨4⟩4. $(end - 1) = ((end - 1) - 1 + 1)$
BY ⟨2⟩13 DEF *end*

⟨4⟩5. $Len(stack') = end - 1$
BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3, ⟨4⟩4, ⟨2⟩13, *SubSeqProperties* DEF *end*
⟨4⟩ QED
BY ⟨2⟩14, ⟨4⟩5
⟨3⟩6. $end \in Nat$
BY ⟨2⟩13 DEF *end*
⟨3⟩ QED
BY ⟨3⟩4, ⟨3⟩5, ⟨3⟩6

⟨2⟩10. SUFFICES
ASSUME $i < N$
PROVE $\land IsAMinCover(QNext, X, Y, Leq)$
$\land PartialNext \cap Patch(kNext) = \{\}$
⟨3⟩1. $(i = N) \lor (i < N)$
BY ⟨2⟩19, ⟨2⟩18 DEF *Collect*, *Expand*, i, *Partial*
⟨3⟩ QED goal from ⟨2⟩8
BY ⟨2⟩9, ⟨2⟩10, ⟨3⟩1

⟨2⟩2. SUFFICES $\land QNext \in$ SUBSET Y
$\land IsACover(QNext, X, Leq)$
$\land Cardinality(QNext) = N$
$\land PartialNext \cap Patch(kNext) = \{\}$
goal from ⟨2⟩10
⟨3⟩ HIDE DEF *QNext*
⟨3⟩1. $IsAMinCover(QNext, X, Y, Leq)$
BY ⟨1⟩3, ⟨1⟩4, ⟨2⟩2,
MinCoverEquivCoverCard, *XYAreFiniteSets*,
ProblemInput, *HaveCardAsCost* DEF N
⟨3⟩ QED
BY ⟨2⟩2, ⟨3⟩1

⟨2⟩11. *Expand*
⟨3⟩1. $\neg(i = N)$
BY ⟨2⟩10, ⟨2⟩17, ⟨1⟩4
⟨3⟩ QED
BY ⟨2⟩19, ⟨3⟩1 DEF *Collect*, i, *end*

⟨2⟩23. $\land PartialE = Partial$
$\land kE = k$
$\land iE = i$
$\land QE = Q$
$\land ymax = Lm[k]$
$\land k \in 1 \,..\, N$

⟨3⟩1. $k \in 1 \,..\, N$
⟨4⟩1. $k = i + 1$

BY DEF k

$\langle 4\rangle 2.\ i \in Nat$

BY $\langle 2\rangle 17$

$\langle 4\rangle 3.\ i < N$

BY $\langle 2\rangle 10$

$\langle 4\rangle 4.\ N \in Nat$

BY $\langle 1\rangle 4$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1, \langle 4\rangle 2, \langle 4\rangle 3, \langle 4\rangle 4$

$\langle 3\rangle$ QED

BY $\langle 3\rangle 1, \langle 2\rangle 18$ DEF $PartialE$, $Partial$, end, kE, k, iE, i, QE, Q, $ymax$

$\langle 2\rangle 26.$ ASSUME

NEW $S \in$ SUBSET Q, NEW yk,
$\wedge\ yk \quad \in BelowAndSuff(ymax,\ Q,\ Y)$
$\wedge\ ymax \notin S$

PROVE

$yk \notin S$

$\langle 3\rangle 9.$ SUFFICES ASSUME $yk \in S$

PROVE FALSE

BY $\langle 3\rangle 9$

$\langle 3\rangle 7.\ ymax \notin S$

BY $\langle 2\rangle 26$

$\langle 3\rangle 14.$ PICK $x :\ x \in Only(ymax,\ Q)$

$\langle 4\rangle 1.\ ymax \in Q$

$\langle 5\rangle 1.\ ymax \in Patch(k)$

BY $\langle 2\rangle 23, \langle 1\rangle 4, \langle 1\rangle 3, PatchSplit$ DEF $ymax$

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$ DEF Q

$\langle 4\rangle$ QED

BY $\langle 2\rangle 12, \langle 4\rangle 1, MinimalHasAllEssential$

$\langle 3\rangle 10.\ \forall\, w \in Q \setminus \{ymax\} :\ \neg Leq[x,\ w]$

BY $\langle 3\rangle 14$ DEF $Only$

$\langle 3\rangle 11.\ yk \in Q \setminus \{ymax\}$

$\langle 4\rangle 1.\ yk \neq ymax$

BY $\langle 3\rangle 9, \langle 3\rangle 7$

$\langle 4\rangle 2.\ yk \in Q$

BY $\langle 3\rangle 9,\ S \subseteq Q$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1, \langle 4\rangle 2$

$\langle 3\rangle 12.\ \neg Leq[x,\ yk]$

BY $\langle 3\rangle 10, \langle 3\rangle 11$

$\langle 3\rangle 13.\ Leq[x,\ yk]$

$\langle 4\rangle 1.\ yk \in BelowAndSuff(ymax,\ Q,\ Y)$

BY $\langle 2\rangle 26$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 3\rangle 14$ DEF *BelowAndSuff*, *ymax*

$\langle 3\rangle$ QED goal from $\langle 3\rangle 9$

BY $\langle 3\rangle 12$, $\langle 3\rangle 13$

$\langle 2\rangle 22$. PICK yk :

$\land\ yk \in BelowAndSuff(Lm[k],\ Q,\ Y)$

$\land\ PartialNext = Partial \cup \{yk\}$

$\land\ yk \notin Partial$

$\langle 3\rangle 2$. PICK $r \in 1\,..\,Len(enum)$:

$PartialNext = PartialE \cup \{enum[r]\}$

$\langle 4\rangle 1$. $stack' = front \circ more$

BY $\langle 2\rangle 11$ DEF *Expand*, *front*, *end*, *more*, *enum*, *succ*, *ymax*, *QE*, *kE*, *iE*, *PartialE*

$\langle 4\rangle 2$. $\land\ front \in Seq(\text{SUBSET}\ Y)$

$\land\ more \in Seq(\text{SUBSET}\ Y)$

BY $\langle 2\rangle 20$, $\langle 2\rangle 21$

$\langle 4\rangle 8$. $\land\ Len(front) \in Nat$

$\land\ Len(more) \in Nat$

$\land\ end \in Nat \setminus \{0\}$

$\land\ siNext \in Nat$

BY $\langle 2\rangle 20$, $\langle 2\rangle 21$, $\langle 2\rangle 13$, $\langle 2\rangle 14$ DEF *end*

$\langle 4\rangle$ USE $\langle 4\rangle 8$

$\langle 4\rangle 3$. $siNext \in 1\,..\,Len(stack')$

BY $\langle 2\rangle 14$

$\langle 4\rangle 4$. $siNext > Len(front)$

$\langle 5\rangle 1$. $Len(front) = end - 1$

BY $\langle 2\rangle 20$

$\langle 5\rangle 2$. $siNext \geq end$

BY $\langle 2\rangle 8$ DEF *end*

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle 5$. $\land\ stack[siNext]' = more[siNext - Len(front)]$

$\land\ siNext \in 1\,..\,(Len(front) + Len(more))$

$\langle 5\rangle 1$. $\land\ Len(stack') = Len(front) + Len(more)$

$\land\ \forall\, j \in 1\,..\,(Len(front) + Len(more))$:

$stack[j]' = \text{IF}\ j \leq Len(front)$

THEN $front[j]$

ELSE $more[j - Len(front)]$

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, *ConcatProperties*

$\langle 5\rangle 2$. $\land\ siNext \in 1\,..\,(Len(front) + Len(more))$

$\land\ \neg(siNext \leq Len(front))$

$\langle 6\rangle 1$. $\neg(siNext \leq Len(front))$

BY $\langle 4\rangle 8$, $\langle 4\rangle 4$

$\langle 6\rangle 2.\ siNext \in 1 \,..\, (Len(front) + Len(more))$

BY $\langle 4\rangle 3$, $\langle 5\rangle 1$, $\langle 4\rangle 4$, $\langle 4\rangle 8$

$\langle 6\rangle$ QED

BY $\langle 6\rangle 1$, $\langle 6\rangle 2$

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle$ DEFINE $r \triangleq siNext - end + 1$

$\langle 4\rangle 6.\ r \in 1 \,..\, Len(enum)$

$\langle 5\rangle 1.$ SUFFICES $r \in$ DOMAIN $more$

BY $\langle 5\rangle 1$ DEF $more$

$\langle 5\rangle 2.\ siNext \in end \,..\, (end + Len(more) - 1)$

$\langle 6\rangle 1.\ siNext \geq end$

BY $\langle 2\rangle 20$, $\langle 2\rangle 8$ DEF end

$\langle 6\rangle 2.\ siNext \in 1 \,..\, (end - 1 + Len(more))$

BY $\langle 4\rangle 5$, $\langle 2\rangle 20$

$\langle 6\rangle$ QED

BY $\langle 6\rangle 1$, $\langle 6\rangle 2$

$\langle 5\rangle 3.\ r \in 1 \,..\, Len(more)$

BY $\langle 5\rangle 2$, $\langle 4\rangle 8$ DEF r

$\langle 5\rangle$ QED

BY $\langle 5\rangle 3$, $\langle 2\rangle 21$

$\langle 4\rangle 7.\ more[r] = PartialE \cup \{enum[r]\}$

BY $\langle 4\rangle 6$ DEF $more$

$\langle 4\rangle 10.\ stack[siNext]' = more[r]$

BY $\langle 4\rangle 5$, $\langle 2\rangle 20$ DEF r

$\langle 4\rangle 9.\ PartialNext = PartialE \cup \{enum[r]\}$

BY $\langle 4\rangle 7$, $\langle 4\rangle 10$ DEF $PartialNext$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 6$, $\langle 4\rangle 9$

$\langle 3\rangle$ DEFINE $yk \triangleq enum[r]$

$\langle 3\rangle 3.\ yk \in BelowAndSuff(Lm[k],\ Q,\ Y)$

$\langle 4\rangle 1.\ IsFiniteSet(succ)$

BY $BelowAndSuffIsFinite$, $XYAreFiniteSets$ DEF $succ$

$\langle 4\rangle 2.\ enum \in Bijection(1 \,..\, Len(enum),\ succ)$

BY $\langle 4\rangle 1$, $EnumerateProperties$ DEF $enum$

$\langle 4\rangle 3.\ r \in$ DOMAIN $enum$

BY $\langle 3\rangle 2$, $\langle 4\rangle 2$ DEF $Bijection$, $Injection$

$\langle 4\rangle 4.\ enum[r] \in succ$

BY $\langle 4\rangle 2$, $\langle 4\rangle 3$ DEF $Bijection$, $Injection$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 4$, $\langle 2\rangle 23$ DEF yk, $succ$

$\langle 3\rangle 4.\ yk \notin Partial$

$\langle 4\rangle 2.\ Partial \cap Patch(k) = \{\}$

BY $\langle 2\rangle 6$, $\langle 2\rangle 16$ DEF $Partial$, k, i

⟨4⟩ DEFINE $S \triangleq Partial$
⟨4⟩4. $ymax \notin S$
⟨5⟩1. $ymax \in Patch(k)$
BY ⟨2⟩23, ⟨1⟩4, ⟨1⟩3, *PatchSplit*
⟨5⟩ QED
BY ⟨4⟩2, ⟨5⟩1
⟨4⟩5. $S \subseteq Q$
BY DEF S, Q
⟨4⟩ QED
BY ⟨4⟩4, ⟨3⟩3, ⟨4⟩5, ⟨2⟩26, ⟨2⟩23 DEF S
⟨3⟩ QED
BY ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨2⟩23

⟨2⟩25. $PartialNext \cap Patch(k+1) = \{\}$
⟨3⟩1. $Partial \cap Patch(k) = \{\}$
BY ⟨2⟩6, ⟨2⟩16 DEF *Partial*, k, i
⟨3⟩2. $PartialNext = Partial \cup \{yk\}$
BY ⟨2⟩22
⟨3⟩3. $Patch(k) = \{ymax\} \cup Patch(k+1)$
BY ⟨2⟩23, ⟨1⟩4, ⟨1⟩3, *PatchSplit*
⟨3⟩4. $Patch(k+1) \subseteq Patch(k)$
BY ⟨3⟩3
⟨3⟩5. $Partial \cap Patch(k+1) = \{\}$
BY ⟨3⟩1, ⟨3⟩4
⟨3⟩6. SUFFICES $yk \notin Patch(k+1)$
BY ⟨3⟩2, ⟨3⟩5
⟨3⟩ QED
⟨4⟩ DEFINE $S \triangleq Patch(k+1)$
⟨4⟩1. $ymax \notin S$
BY ⟨1⟩3, ⟨2⟩23, *PatchSplit* DEF S
⟨4⟩2. $S \in$ SUBSET Q
BY ⟨3⟩4 DEF S, Q
⟨4⟩3. $yk \in BelowAndSuff(ymax, Q, Y)$
BY ⟨2⟩22, ⟨2⟩23
⟨4⟩ QED goal from ⟨3⟩6
BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3, ⟨2⟩26

⟨2⟩24. $\wedge\ iNext \in Nat$
$\wedge\ kNext \in Nat$
$\wedge\ k \in Nat$
$\wedge\ kNext = k+1$
$\wedge\ IsFiniteSet(PartialNext)$
$\wedge\ Cardinality(PartialNext) = k$
⟨3⟩1. $IsFiniteSet(Partial)$
⟨4⟩ DEFINE $S \triangleq$ DOMAIN *stack*

⟨4⟩1. $Partial = stack[si]$
BY DEF $Partial$
⟨4⟩2. $stack[si] \subseteq Y$
⟨5⟩1. $si \in S$
BY ⟨2⟩16 DEF S
⟨5⟩2. $stack \in [S \to \text{SUBSET } Y]$
BY ⟨2⟩13 DEF S
⟨5⟩ QED
BY ⟨5⟩1, ⟨5⟩2
⟨4⟩3. $Partial \subseteq Y$
BY ⟨4⟩1, ⟨4⟩2
⟨4⟩4. $IsFiniteSet(Y)$
BY $XYAreFiniteSets$
⟨4⟩ QED
BY ⟨4⟩3, ⟨4⟩4, FS_Subset
⟨3⟩2. $yk \notin Partial$
BY ⟨2⟩22
⟨3⟩3. $\land\ IsFiniteSet(Partial \cup \{yk\})$
$\land\ Cardinality(Partial \cup \{yk\}) = i + 1$
BY ⟨3⟩1, ⟨3⟩2, $FS\_AddElement$ DEF i
⟨3⟩4. $\land\ IsFiniteSet(PartialNext)$
$\land\ Cardinality(PartialNext) = i + 1$
BY ⟨3⟩3, ⟨2⟩22
⟨3⟩5. $\land\ iNext = i + 1$
$\land\ iNext \in Nat$
BY ⟨3⟩4, ⟨2⟩17 DEF $iNext$
⟨3⟩6. $\land\ kNext = k + 1$
$\land\ kNext \in Nat$
$\land\ k \in Nat$
⟨4⟩1. $\land\ kNext = iNext + 1$
$\land\ k = i + 1$
BY DEF $kNext$, k
⟨4⟩ QED
BY ⟨4⟩1, ⟨3⟩5, ⟨2⟩17
⟨3⟩ QED
BY ⟨3⟩4, ⟨3⟩5, ⟨3⟩6 DEF k

⟨2⟩3. $QNext \in \text{SUBSET } Y$
⟨3⟩1. $QNext = PartialNext \cup Patch(kNext)$
BY DEF $QNext$
⟨3⟩2. $PartialNext \in \text{SUBSET } Y$
⟨4⟩1. $PartialNext = Partial \cup \{yk\}$
BY ⟨2⟩22
⟨4⟩2. $Partial \in \text{SUBSET } Y$
⟨5⟩1. $Partial \subseteq Q$

BY DEF Q

$\langle 5\rangle 2.\ Q \subseteq Y$

BY $\langle 2\rangle 12$

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle 3.\ yk \in Y$

BY $\langle 2\rangle 22$ DEF *BelowAndSuff*

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$

$\langle 3\rangle 3.\ Patch(kNext) \in$ SUBSET Y

BY $\langle 2\rangle 24$, $\langle 1\rangle 3$, $\langle 1\rangle 4$, $\langle 2\rangle 23$, *PatchProperties*

$\langle 3\rangle$ QED

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

$\langle 2\rangle 4.\ IsACover(QNext,\ X,\ Leq)$

$\langle 3\rangle 1.$ SUFFICES

ASSUME NEW $x \in X$

PROVE $\exists\, y \in QNext :\ Leq[x,\ y]$

BY $\langle 3\rangle 1$ DEF *IsACover*

$\langle 3\rangle 2.$CASE $\exists\, y \in Q \setminus \{ymax\} :\ Leq[x,\ y]$

$\langle 4\rangle 1.$ PICK $y \in Q \setminus \{ymax\} :\ Leq[x,\ y]$

BY $\langle 3\rangle 2$

If y is an element from Q other than yk,
then it belongs to the intersection of Q and $QNext$.

$\langle 4\rangle 2.$ SUFFICES $y \in QNext$

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$

$\langle 4\rangle 3.\ \wedge\ y \in Partial \cup Patch(k)$
$\quad\ \wedge\ y \neq ymax$

BY $\langle 4\rangle 1$ DEF Q

$\langle 4\rangle 4.\ Patch(k) = (Patch(kNext) \cup \{ymax\})$

$\langle 5\rangle 1.\ Patch(k) = (Patch(k+1) \cup \{ymax\})$

$\langle 6\rangle 1.\ N \in Nat$

BY $\langle 1\rangle 4$

$\langle 6\rangle 2.\ k \in 1\,..\,N$

BY $\langle 2\rangle 23$

$\langle 6\rangle 3.\ ymax = Lm[k]$

BY $\langle 2\rangle 23$ DEF $ymax$

$\langle 6\rangle$ QED

BY $\langle 6\rangle 1$, $\langle 6\rangle 2$, $\langle 6\rangle 3$, $\langle 2\rangle 23$,
$\langle 1\rangle 3$, $\langle 1\rangle 4$, *PatchSplit*

$\langle 5\rangle 2.\ kNext = k+1$

BY $\langle 2\rangle 24$

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle 5.\ y \in Partial \cup Patch(kNext)$

BY $\langle 4\rangle 3$, $\langle 4\rangle 4$

$\langle 4\rangle 6.\ (Partial \cup Patch(kNext)) \subseteq QNext$

$\langle 5\rangle 1.\ PartialNext = Partial \cup \{yk\}$

BY $\langle 2\rangle 22$

$\langle 5\rangle 2.\ QNext = PartialNext \cup Patch(kNext)$

BY DEF $QNext$

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 5$, $\langle 4\rangle 6$

$\langle 3\rangle 3.$CASE $\forall\, y \in Q \setminus \{ymax\} :\ \neg Leq[x,\ y]$

$\langle 4\rangle 1.$ SUFFICES $Leq[x,\ yk]$ goal from $\langle 3\rangle 1$

$\langle 5\rangle 1.\ yk \in QNext$

$\langle 6\rangle 1.\ yk \in PartialNext$

BY $\langle 2\rangle 22$

$\langle 6\rangle 2.\ PartialNext \subseteq QNext$

BY DEF $QNext$

$\langle 6\rangle$ QED

BY $\langle 6\rangle 1$, $\langle 6\rangle 2$

$\langle 5\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 2\rangle 22$, $\langle 5\rangle 1$

If x is in the k-th gap, then yk covers it,
because yk was selected to have this property, via *BelowAndSuff*.

$\langle 4\rangle 2.\ x \in Only(ymax,\ Q)$

BY $\langle 3\rangle 1$, $\langle 3\rangle 3$ DEF $Only$

$\langle 4\rangle 3.$ $\land\, yk \in Y$
$\land\, yk \in Leq[y,\ ymax]$
$\forall\, u \in Only(ymax,\ Q) :\ Leq[u,\ yk]$

$\langle 5\rangle 1.\ yk \in BelowAndSuff(ymax,\ Q,\ Y)$

BY $\langle 2\rangle 22$, $\langle 2\rangle 23$ DEF $ymax$

$\langle 5\rangle$ QED

BY $\langle 5\rangle 1$ DEF $BelowAndSuff$

$\langle 4\rangle$ QED goal from $\langle 4\rangle 1$

BY $\langle 4\rangle 2$, $\langle 4\rangle 3$

$\langle 3\rangle$ QED goal from $\langle 3\rangle 1$

BY $\langle 3\rangle 2$, $\langle 3\rangle 3$

$\langle 2\rangle 5.\ Cardinality(QNext) = N$

$\langle 3\rangle$ DEFINE $Pc \triangleq Patch(kNext)$

$\langle 3\rangle 8.$ $\land\, N \in Nat$
$\land\, k \in Nat$

BY $\langle 1\rangle 4$, $\langle 2\rangle 24$

$\langle 3\rangle 1.\ QNext = PartialNext \cup Pc$

BY DEF $QNext$, Pc

⟨3⟩6. $Cardinality(QNext) = Cardinality(PartialNext) + Cardinality(Pc) - Cardinality(PartialNext \cap Pc)$
⟨4⟩1. $IsFiniteSet(PartialNext)$
BY ⟨2⟩24
⟨4⟩2. $IsFiniteSet(Pc)$
⟨5⟩1. $kNext \in 1 \,..\, (N+1)$
BY ⟨2⟩23, ⟨2⟩24, ⟨1⟩4
⟨5⟩2. $Cm \in \text{SUBSET } Y$
BY ⟨1⟩3
⟨5⟩ QED
BY ⟨5⟩1, ⟨5⟩2, *PatchProperties* DEF Pc
⟨4⟩ QED
BY ⟨3⟩1, ⟨4⟩1, ⟨4⟩2, *FS_Union*
⟨3⟩2. $Cardinality(PartialNext \cap Pc) = 0$
⟨4⟩1. $PartialNext \cap Pc = \{\}$
BY ⟨2⟩25, ⟨2⟩24 DEF Pc
⟨4⟩ QED
BY ⟨4⟩1, *FS_EmptySet*
⟨3⟩3. $Cardinality(PartialNext) = k$
BY ⟨2⟩24
⟨3⟩4. $Cardinality(Pc) = N - k$
⟨4⟩1. $kNext = k + 1$
BY ⟨2⟩24
⟨4⟩2. $Cardinality(Pc) = N - kNext + 1$
⟨5⟩1. $kNext \in 1 \,..\, (N \ \ + 1)$
BY ⟨2⟩23, ⟨2⟩24, ⟨1⟩4
⟨5⟩2. $Cm \in \text{SUBSET } Y$
BY ⟨1⟩3
⟨5⟩ QED
BY ⟨5⟩1, ⟨5⟩2, *PatchProperties* DEF Pc
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩2, ⟨3⟩8
⟨3⟩ QED
BY ⟨3⟩6, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩8

⟨2⟩ QED goal from ⟨2⟩2
BY ⟨2⟩3, ⟨2⟩4, ⟨2⟩5, ⟨2⟩25, ⟨2⟩24
⟨1⟩5. ASSUME $PartialCoversInStack \land$ UNCHANGED $vars$
PROVE $PartialCoversInStack'$
BY ⟨1⟩5 DEF $PartialCoversInStack$, $vars$
⟨1⟩6. ASSUME $[TypeInv \land TypeInv' \land Next]_{vars} \land PartialCoversInStack$
PROVE $PartialCoversInStack'$
BY ⟨1⟩2, ⟨1⟩5, ⟨1⟩6
⟨1⟩ DEFINE
$Inv \triangleq PartialCoversInStack$

$Nx \triangleq TypeInv \land TypeInv' \land Next$

⟨1⟩7. ASSUME $Inv \land [Nx]_{vars}$
PROVE Inv'
BY ⟨1⟩6, ⟨1⟩7 DEF Inv, Nx

⟨1⟩ QED
⟨2⟩1. $\lor \neg \land PartialCoversInStack$
$\land \Box[TypeInv \land TypeInv' \land Next]_{vars}$
$\lor \Box PartialCoversInStack$
BY ⟨1⟩7, PTL DEF Inv, Nx *RuleINV1*
⟨2⟩2. $\lor \neg \land Init$
$\land \Box[TypeInv \land TypeInv' \land Next]_{vars}$
$\lor \Box PartialCoversInStack$
BY ⟨1⟩1, ⟨2⟩1
⟨2⟩3. $\lor \neg \land Init$
$\land \Box TypeInv$
$\land \Box[Next]_{vars}$
$\lor \Box PartialCoversInStack$
BY ⟨2⟩2, PTL *RuleINV2*
⟨2⟩ QED
BY ⟨2⟩3, $TypeOK$, PTL DEF $Spec$

We now show that:
$MinCoversBelow(Cm) \subseteq MinCoversOf(X, Y, Leq)$

THEOREM $StrongReductionSoundness \triangleq$
ASSUME
NEW C,
$IsAMinCover(Cm, X, Max, Leq)$
PROVE
$Spec \Rightarrow \Box InvSound(C)$
PROOF
⟨1⟩1. ASSUME $Init$
PROVE $InvSound(C)$
⟨2⟩1. $MinCoversBelow = \{\}$
BY ⟨1⟩1 DEF $Init$
⟨2⟩ QED
BY ⟨2⟩1 DEF $InvSound$
⟨1⟩2. ASSUME $TypeInv \land PartialCoversInStack \land Next \land InvSound(C)$
PROVE $InvSound(C)'$
⟨2⟩1. $\land stack \neq \langle\rangle$
$\land Collect \lor Expand$
BY ⟨1⟩2 DEF $Next$
⟨2⟩2.CASE $Expand$
BY ⟨1⟩2, ⟨2⟩2 DEF $Expand$, $InvSound$
⟨2⟩3.CASE $Collect$

⟨3⟩5. SUFFICES ASSUME $C \in MinCoversBelow'$
PROVE $IsAMinCover(C,\ X,\ Y,\ Leq)$
BY ⟨3⟩5 DEF $InvSound$
⟨3⟩ DEFINE
$end \triangleq Len(stack)$
$Partial \triangleq stack[end]$
$i \triangleq Cardinality(Partial)$
$k \triangleq i + 1$
$Q \triangleq Partial \cup Patch(k)$
⟨3⟩8. $end \in$ DOMAIN $stack$
⟨4⟩4. $stack \in Seq($SUBSET $Y)$
BY ⟨1⟩2 DEF $TypeInv$
⟨4⟩1. $\wedge\ Len(stack) \in Nat$
$\wedge$ DOMAIN $stack = 1\ ..\ Len(stack)$
BY ⟨4⟩4, $LenProperties$
⟨4⟩2. $\wedge\ end \in Nat$
$\wedge\ end \in 1\ ..\ end$
BY ⟨4⟩1, ⟨2⟩1, ⟨4⟩4, $EmptySeq$ DEF end
⟨4⟩3. $end \in 1\ ..\ Len(stack)$
BY ⟨4⟩2 DEF end
⟨4⟩ QED
BY ⟨4⟩1, ⟨4⟩3
⟨3⟩7. $\wedge\ i \in Nat$
$\wedge\ k \in Nat$
$\wedge\ N \in Nat$
⟨4⟩1. $stack \in Seq($SUBSET $Y)$
BY ⟨1⟩2 DEF $TypeInv$
⟨4⟩2. $Partial \in$ SUBSET Y
BY ⟨4⟩1, ⟨3⟩8, $LenProperties$ DEF $Partial$
⟨4⟩3. $IsFiniteSet(Partial)$
BY ⟨4⟩2, $SubsetYFinite$
⟨4⟩4. $i \in Nat$
BY ⟨4⟩3, $FS\_CardinalityType$ DEF i
⟨4⟩5. $k \in Nat$
BY ⟨4⟩4 DEF k
⟨4⟩6. $N \in Nat$
BY $MinCoverFromMaxYIsMinCoverFromY$,
$MinCoverProperties$, $NType$
⟨4⟩ QED
BY ⟨4⟩4, ⟨4⟩5, ⟨4⟩6
⟨3⟩1. $\wedge\ i = N$
$\wedge\ MinCoversBelow' = MinCoversBelow \cup \{Partial\}$
BY ⟨2⟩3 DEF $Collect$, i, $Partial$, end
⟨3⟩2. $IsAMinCover(Q,\ X,\ Y,\ Leq)$
BY ⟨3⟩8, ⟨1⟩2 DEF $PartialCoversInStack$,

Q, $Partial$, end, k, i

$\langle 3\rangle 3.\ Q = Partial$

$\langle 4\rangle 1.\ k = N + 1$

BY $\langle 3\rangle 7$, $\langle 3\rangle 1$ DEF k

$\langle 4\rangle 2.\ Patch(k) = \{\}$

BY $\langle 4\rangle 1$, $\langle 3\rangle 7$ DEF $Patch$, $Image$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 2$ DEF Q

$\langle 3\rangle 4.$CASE $C \in MinCoversBelow$

BY $\langle 1\rangle 2$, $\langle 3\rangle 4$ DEF $InvSound$

$\langle 3\rangle 6.$CASE $C \notin MinCoversBelow$

$\langle 4\rangle 1.\ C = Partial$

BY $\langle 3\rangle 6$, $\langle 3\rangle 5$, $\langle 3\rangle 1$

$\langle 4\rangle$ QED

BY $\langle 4\rangle 1$, $\langle 3\rangle 3$, $\langle 3\rangle 2$

$\langle 3\rangle$ QED

BY $\langle 3\rangle 4$, $\langle 3\rangle 6$

$\langle 2\rangle$ QED

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

$\langle 1\rangle 3.$ ASSUME $[TypeInv \land PartialCoversInStack \land Next]_{vars} \land InvSound(C)$

PROVE $InvSound(C)'$

BY $\langle 1\rangle 2$, $\langle 1\rangle 3$ DEF $InvSound$, $vars$

$\langle 1\rangle$ DEFINE

$Inv \triangleq InvSound(C)$

$Nxt \triangleq TypeInv \land PartialCoversInStack \land Next$

$\langle 1\rangle 4.$ ASSUME $Inv \land [Nxt]_{vars}$

PROVE Inv'

BY $\langle 1\rangle 3$, $\langle 1\rangle 4$ DEF Inv, Nxt, $InvSound$, $vars$

$\langle 1\rangle$ QED

$\langle 2\rangle 4.\ (Inv \land \Box[Nxt]_{vars}) \Rightarrow \Box Inv$

BY $\langle 1\rangle 4$, PTL $RuleINV1$

$\langle 2\rangle 1.\ \lor \neg \land InvSound(C)$

$\land \Box[TypeInv \land PartialCoversInStack \land Next]_{vars}$

$\lor \Box InvSound(C)$

BY $\langle 2\rangle 4$ DEF Inv, Nxt

$\langle 2\rangle 2.\ \lor \neg \land Init$

$\land \Box[TypeInv \land PartialCoversInStack \land Next]_{vars}$

$\lor \Box InvSound(C)$

BY $\langle 1\rangle 1$, $\langle 2\rangle 1$

$\langle 2\rangle 3.\ \lor \neg \land Init$

$\land \Box TypeInv$

$\land \Box PartialCoversInStack$

$\land \Box[Next]_{vars}$

$\lor \Box InvSound(C)$

BY $\langle 2\rangle 2$, PTL $RuleINV2$

⟨2⟩ QED
BY ⟨2⟩3, *StackContainsPartialCovers*, *TypeOK*, *PTL* DEF *Spec*

THEOREM *StrongReductionSafety* $\triangleq$
ASSUME
NEW C,
$IsAMinCover(Cm,\ X,\ Max,\ Leq)$
PROVE
$\land\ Spec \Rightarrow \Box InvSound(C)$
$\land\ (C \in AllCandidatesBelow(Cm,\ Y))$
$\Rightarrow (Spec \Rightarrow \Box InvCompl(C))$
PROOF
⟨1⟩1. ASSUME $C \in AllCandidatesBelow(Cm,\ Y)$
PROVE $C \in \text{SUBSET } Y$
BY ⟨1⟩1 DEF *AllCandidatesBelow*
⟨1⟩ QED
BY ⟨1⟩1, *StrongReductionSoundness*, *StrongReductionCompleteness*

(* Proofs checked with *TLAPS* version 1.4.3 *)