Minimal CBC Casper Isabelle/HOL proofs

LayerX

February 19, 2019

Contents

1 Description of CBC Casper 1

2 Safety Proof 11

3 Latest Message 16

1 Description of CBC Casper

theory *CBCCasper*

imports *Main HOL.Real AFP/Restricted-Predicates*

begin

notation *Set.empty* (∅)

typedecl *validator*

typedecl *consensus-value*

datatype *message* =
  Message consensus-value ∗ *validator* ∗ *message list*

type-synonym *state* = *message set*

fun *sender* :: *message* ⇒ *validator*
  where
    sender (*Message* (-, *v*, -)) = *v*

fun *est* :: *message* ⇒ *consensus-value*
  where
    est (*Message* (*c*, -, -)) = *c*

fun *justification* :: *message* ⇒ *state*
  where
    justification (*Message* (-, -, *s*)) = *set s*

fun
  Σ-*i* :: (*validator set* × *consensus-value set* × (*message set* ⇒ *consensus-value set*)) ⇒ *nat* ⇒ *state set* **and**
  M-i :: (*validator set* × *consensus-value set* × (*message set* ⇒ *consensus-value set*)) ⇒ *nat* ⇒ *message set*
  where
    Σ-*i* (*V*,*C*,ε) *0* = {∅}
  | Σ-*i* (*V*,*C*,ε) *n* = {σ ∈ *Pow* (*M-i* (*V*,*C*,ε) (*n* − *1*)). *finite* σ ∧ (∀ *m*. *m* ∈ σ ⟶ *justification m* ⊆ σ)}
  | *M-i* (*V*,*C*,ε) *n* = {*m*. *est m* ∈ *C* ∧ *sender m* ∈ *V* ∧ *justification m* ∈ (Σ-*i* (*V*,*C*,ε) *n*) ∧ *est m* ∈ ε (*justification m*)}

locale *Params* =
  fixes *V* :: *validator set*
  and *W* :: *validator* ⇒ *real*
  and *t* :: *real*
  fixes *C* :: *consensus-value set*
  and ε :: *message set* ⇒ *consensus-value set*

begin
  definition Σ = (⋃ *i*∈ℕ. Σ-*i* (*V*,*C*,ε) *i*)
  definition *M* = (⋃ *i*∈ℕ. *M-i* (*V*,*C*,ε) *i*)
  definition *is-valid-estimator* :: (*state* ⇒ *consensus-value set*) ⇒ *bool*
    where
      is-valid-estimator e = (∀ σ ∈ Σ. *e* σ ∈ *Pow C* − {∅})

  lemma Σ*i-subset-Mi*: Σ-*i* (*V*,*C*,ε) (*n* + *1*) ⊆ *Pow* (*M-i* (*V*,*C*,ε) *n*)
    by *force*

  lemma Σ*i-subset-to-Mi*: Σ-*i* (*V*,*C*,ε) *n* ⊆ Σ-*i* (*V*,*C*,ε) (*n*+*1*) ⟹ *M-i* (*V*,*C*,ε) *n* ⊆ *M-i* (*V*,*C*,ε) (*n*+*1*)
    by *auto*

  lemma *Mi-subset-to-*Σ*i*: *M-i* (*V*,*C*,ε) *n* ⊆ *M-i* (*V*,*C*,ε) (*n*+*1*) ⟹ Σ-*i* (*V*,*C*,ε)

$(n+1) \subseteq \Sigma\text{-}i\ (V,C,\varepsilon)\ (n+2)$
by *auto*

lemma *Σi-monotonic*: $\Sigma\text{-}i\ (V,C,\varepsilon)\ n \subseteq \Sigma\text{-}i\ (V,C,\varepsilon)\ (n+1)$
apply (*induction n*)
apply *simp*
apply (*metis Mi-subset-to-Σi Suc-eq-plus1 Σi-subset-to-Mi add.commute add-2-eq-Suc*)
done

lemma *Mi-monotonic*: $M\text{-}i\ (V,C,\varepsilon)\ n \subseteq M\text{-}i\ (V,C,\varepsilon)\ (n+1)$
apply (*induction n*)
defer
using *Σi-monotonic Σi-subset-to-Mi* **apply** *blast*
apply *auto*
done

lemma *message-is-in-M-i* :
$\forall\ m \in M.\ \exists\ n \in \mathbb{N}.\ m \in M\text{-}i\ (V,\ C,\ \varepsilon)\ (n - 1)$
apply (*simp add*: *M-def Σ-i.elims*)
by (*metis Nats-1 Nats-add One-nat-def diff-Suc-1 plus-1-eq-Suc*)

lemma *state-is-in-pow-M-i* :
$\forall\ \sigma \in \Sigma.\ (\exists\ n \in \mathbb{N}.\ \sigma \in Pow\ (M\text{-}i\ (V,\ C,\ \varepsilon)\ (n - 1)) \wedge (\forall\ m \in \sigma.\ justification\ m \subseteq \sigma))$
apply (*simp add*: *Σ-def*)

apply *auto*
proof −
fix y :: *nat* **and** σ :: *message set*
assume *a1*: $\sigma \in \Sigma\text{-}i\ (V,\ C,\ \varepsilon)\ y$
assume *a2*: $y \in \mathbb{N}$
have $\sigma \subseteq M\text{-}i\ (V,\ C,\ \varepsilon)\ y$
using *a1* **by** (*meson Params.Σi-monotonic Params.Σi-subset-Mi Pow-iff contra-subsetD*)
then have $\exists n.\ n \in \mathbb{N} \wedge \sigma \subseteq M\text{-}i\ (V,\ C,\ \varepsilon)\ (n - 1)$
using *a2* **by** (*metis* (*no-types*) *Nats-1 Nats-add diff-Suc-1 plus-1-eq-Suc*)
then show $\exists n{\in}\mathbb{N}.\ \sigma \subseteq \{m.\ est\ m \in C \wedge sender\ m \in V \wedge justification\ m \in \Sigma\text{-}i\ (V,\ C,\ \varepsilon)\ (n - Suc\ 0) \wedge est\ m \in \varepsilon\ (justification\ m)\}$
by *auto*
next
show $\bigwedge y\ \sigma\ m\ x.\ y \in \mathbb{N} \Longrightarrow \sigma \in \Sigma\text{-}i\ (V,\ C,\ \varepsilon)\ y \Longrightarrow m \in \sigma \Longrightarrow x \in justification\ m \Longrightarrow x \in \sigma$
using *Params.Σi-monotonic* **by** *fastforce*
qed

lemma *message-is-in-M-i-n* :
$\forall\ m \in M.\ \exists\ n \in \mathbb{N}.\ m \in M\text{-}i\ (V,\ C,\ \varepsilon)\ n$
by (*smt Mi-monotonic Suc-diff-Suc add-leE diff-add diff-le-self message-is-in-M-i*

neq0-conv plus-1-eq-Suc subsetCE zero-less-diff)

lemma *message-in-state-is-valid* :
$\forall\ \sigma\ m.\ \sigma \in \Sigma \wedge m \in \sigma \longrightarrow\ m \in M$
apply (*rule*, *rule*, *rule*)
proof −
fix $\sigma\ m$
assume $\sigma \in \Sigma \wedge m \in \sigma$
have
$\exists\ n \in \mathbb{N}.\ m \in M\text{-}i\ (V,\ C,\ \varepsilon)\ n$
$\Longrightarrow m \in M$
using *M-def* **by** *blast*
then show
$m \in M$
apply (*simp add*: *M-def*)
by (*smt M-i.simps Params.Σi-monotonic PowD Suc-diff-Suc* ‹$\sigma \in \Sigma \wedge m \in \sigma$› *add-leE diff-add diff-le-self gr0I mem-Collect-eq plus-1-eq-Suc state-is-in-pow-M-i subsetCE zero-less-diff*)
qed

lemma *state-is-subset-of-M* : $\forall\ \sigma \in \Sigma.\ \sigma \subseteq M$
using *message-in-state-is-valid* **by** *blast*

lemma *state-difference-is-valid-message* :
$\forall\ \sigma\ \sigma'.\ \sigma \in \Sigma \wedge \sigma' \in \Sigma$
$\longrightarrow$ *is-future-state*$(\sigma',\ \sigma)$
$\longrightarrow \sigma' - \sigma \subseteq M$
using *state-is-subset-of-M* **by** *blast*

lemma *state-is-finite* : $\forall\ \sigma \in \Sigma.$ *finite* σ
apply (*simp add*: Σ-*def*)
using *Params.Σi-monotonic* **by** *fastforce*

lemma *justification-is-finite* : $\forall\ m \in M.$ *finite* (*justification* m)
apply (*simp add*: *M-def*)
using *Params.Σi-monotonic* **by** *fastforce*

lemma Σ-*is-subseteq-of-pow-M*: $\Sigma \subseteq Pow\ M$
by (*simp add*: *state-is-subset-of-M subsetI*)

lemma *M-type*: $\bigwedge m.\ m \in M \Longrightarrow est\ m \in C \wedge sender\ m \in V \wedge justification\ m \in \Sigma$
unfolding *M-def* Σ-*def*
by *auto*

end

locale *Protocol* = *Params* +

assumes *V-type*: $V \neq \emptyset$
and *W-type*: $\bigwedge w.\ w \in range\ W \Longrightarrow w > 0$
and *t-type*: $0 \leq t\ t < Sum\ (W\ `\ V)$
and *C-type*: $card\ C > 1$
and *ε-type*: *is-valid-estimator* ε

lemma (**in** *Protocol*) *estimates-are-non-empty*: $\bigwedge \sigma.\ \sigma \in \Sigma \Longrightarrow \varepsilon\ \sigma \neq \emptyset$
using *is-valid-estimator-def ε-type* **by** *auto*

lemma (**in** *Protocol*) *estimates-are-subset-of-C*: $\bigwedge \sigma.\ \sigma \in \Sigma \Longrightarrow \varepsilon\ \sigma \subseteq C$
using *is-valid-estimator-def ε-type* **by** *auto*

lemma (**in** *Params*) *empty-set-exists-in-Σ-0*: $\emptyset \in \Sigma\text{-}i\ (V,\ C,\ \varepsilon)\ 0$
by *simp*

lemma (**in** *Params*) *empty-set-exists-in-Σ*: $\emptyset \in \Sigma$
apply (*simp add*: *Σ-def*)
using *Nats-0 Σ-i.simps(1)* **by** *blast*

lemma (**in** *Params*) *Σ-i-is-non-empty*: $\Sigma\text{-}i\ (V,\ C,\ \varepsilon)\ n \neq \emptyset$
apply (*induction n*)
using *empty-set-exists-in-Σ-0* **by** *auto*

lemma (**in** *Params*) *Σ-is-non-empty*: $\Sigma \neq \emptyset$
using *empty-set-exists-in-Σ* **by** *blast*

lemma (**in** *Protocol*) *estimates-exists-for-empty-set* :
$\varepsilon\ \emptyset \neq \emptyset$
by (*simp add*: *empty-set-exists-in-Σ estimates-are-non-empty*)

lemma (**in** *Protocol*) *non-justifying-message-exists-in-M-0*:
$\exists\ m.\ m \in M\text{-}i\ (V,\ C,\ \varepsilon)\ 0 \wedge justification\ m = \emptyset$
apply *auto*
proof −
have $\varepsilon\ \emptyset \subseteq C$
using *Params.empty-set-exists-in-Σ ε-type is-valid-estimator-def* **by** *auto*
then show $\exists m.\ est\ m \in C \wedge sender\ m \in V \wedge justification\ m = \emptyset \wedge est\ m \in \varepsilon\ (justification\ m) \wedge justification\ m = \emptyset$
by (*metis V-type all-not-in-conv est.simps estimates-exists-for-empty-set justification.simps sender.simps set-empty subsetCE*)
qed

lemma (**in** *Protocol*) *M-i-is-non-empty*: $M\text{-}i\ (V,\ C,\ \varepsilon)\ n \neq \emptyset$
apply (*induction n*)
using *non-justifying-message-exists-in-M-0* **apply** *auto*
using *Mi-monotonic empty-iff empty-subsetI* **by** *fastforce*

lemma (**in** *Protocol*) *M-is-non-empty*: $M \neq \emptyset$
using *non-justifying-message-exists-in-M-0 M-def Nats-0* **by** *blast*

lemma (**in** *Protocol*) *C-is-not-empty* : $C \neq \emptyset$
  using *C-type* **by** *auto*

lemma (**in** *Params*) Σ*i-is-subset-of-*Σ :
  $\forall\ n \in \mathbb{N}.\ \Sigma\text{-}i\ (V,\ C,\ \varepsilon)\ n \subseteq \Sigma$
  by (*simp add*: Σ*-def SUP-upper*)

lemma (**in** *Protocol*) *message-justifying-state-in-*Σ*-n-exists-in-M-n* :
  $\forall\ n \in \mathbb{N}.\ (\forall\ \sigma.\ \sigma \in \Sigma\text{-}i\ (V,\ C,\ \varepsilon)\ n \longrightarrow (\exists\ m.\ m \in M\text{-}i\ (V,\ C,\ \varepsilon)\ n\ \wedge$ *justification* $m = \sigma))$
  apply *auto*
proof –
  fix $n\ \sigma$
  assume $n \in \mathbb{N}$
  and $\sigma \in \Sigma\text{-}i\ (V,\ C,\ \varepsilon)\ n$
  then have $\sigma \in \Sigma$
    using Σ*i-is-subset-of-*Σ **by** *auto*
  have $\varepsilon\ \sigma \neq \emptyset$
    using *estimates-are-non-empty* $\langle\sigma \in \Sigma\rangle$ **by** *auto*
  have *finite* σ
    using *state-is-finite* $\langle\sigma \in \Sigma\rangle$ **by** *auto*
  moreover have $\exists\ m.$ *sender* $m \in V\ \wedge$ *est* $m \in \varepsilon\ \sigma\ \wedge$ *justification* $m = \sigma$
    using *est.simps sender.simps justification.simps V-type* $\langle\varepsilon\ \sigma \neq \emptyset\rangle$ $\langle$*finite* $\sigma\rangle$
    by (*metis all-not-in-conv finite-list*)
  moreover have $\varepsilon\ \sigma \subseteq C$
    using *estimates-are-subset-of-C* Σ*i-is-subset-of-*Σ $\langle n \in \mathbb{N}\rangle$ $\langle\sigma \in \Sigma\text{-}i\ (V,\ C,\ \varepsilon)\ n\rangle$ **by** *blast*
  ultimately show $\exists\ m.$ *est* $m \in C\ \wedge$ *sender* $m \in V\ \wedge$ *justification* $m \in \Sigma\text{-}i\ (V,\ C,\ \varepsilon)\ n\ \wedge$ *est* $m \in \varepsilon$ (*justification* m) $\wedge$ *justification* $m = \sigma$
    using *Nats-1 One-nat-def*
    using $\langle\sigma \in \Sigma\text{-}i\ (V,\ C,\ \varepsilon)\ n\rangle$ **by** *blast*
qed

lemma (**in** *Protocol*) Σ*-type*: $\Sigma \subset$ *Pow M*
proof –
  obtain m **where** $m \in M\text{-}i\ (V,\ C,\ \varepsilon)\ 0\ \wedge$ *justification* $m = \emptyset$
    using *non-justifying-message-exists-in-M-0* **by** *auto*
  then have $\{m\} \in \Sigma\text{-}i\ (V,\ C,\ \varepsilon)\ (Suc\ 0)$
    using *Params.*Σ*i-subset-Mi* **by** *auto*
  then have $\exists\ m'.\ m' \in\ M\text{-}i\ (V,\ C,\ \varepsilon)\ (Suc\ 0)\ \wedge$ *justification* $m' = \{m\}$
    using *message-justifying-state-in-*Σ*-n-exists-in-M-n Nats-1 One-nat-def* **by** *metis*
  then obtain m' **where** $m' \in\ M\text{-}i\ (V,\ C,\ \varepsilon)\ (Suc\ 0)\ \wedge$ *justification* $m' = \{m\}$ **by** *auto*
  then have $\{m'\} \in$ *Pow M*
    using *M-def*
    by (*metis Nats-1 One-nat-def PowD PowI Pow-bottom UN-I insert-subset*)
  moreover have $\{m'\} \notin \Sigma$

using *Params.state-is-in-pow-M-i Protocol-axioms* ‹$m' \in$ *M-i* $(V,\ C,\ \varepsilon)$ (*Suc 0*) $\wedge$ *justification* $m' = \{m\}$› **by** *fastforce*
ultimately show *?thesis*
using Σ*-is-subseteq-of-pow-M* **by** *auto*
qed

lemma (**in** *Protocol*) *M-type-counterexample*:
$(\forall\ \sigma.\ \varepsilon\ \sigma = C) \Longrightarrow M = \{m.\ est\ m \in C \wedge sender\ m \in V \wedge justification\ m \in \Sigma\}$
apply (*simp add*: *M-def*)
apply *auto*
using Σ*i-is-subset-of-*Σ **apply** *blast*
by (*simp add*: Σ*-def*)

definition *observed* :: *state* $\Rightarrow$ *validator set*
where
observed $\sigma = \{sender\ m \mid m.\ m \in \sigma\}$

lemma (**in** *Protocol*) *observed-type* :
$\forall\ \sigma \in \Sigma.\ observed\ \sigma \subseteq V$
using *Params.M-type Protocol-axioms observed-def state-is-subset-of-M* **by** *fastforce*

fun *is-future-state* :: (*state* $*$ *state*) $\Rightarrow$ *bool*
where
is-future-state $(\sigma 1,\ \sigma 2) = (\sigma 1 \supseteq \sigma 2)$

definition *justified* :: *message* $\Rightarrow$ *message* $\Rightarrow$ *bool*
where
justified m1 m2 = (*m1* $\in$ *justification m2*)

definition *equivocation* :: (*message* $*$ *message*) $\Rightarrow$ *bool*
where
equivocation =
$(\lambda(m1,\ m2).\ sender\ m1 = sender\ m2 \wedge m1 \neq m2 \wedge \neg\ (justified\ m1\ m2) \wedge \neg\ (justified\ m2\ m1))$

definition *is-equivocating* :: *state* $\Rightarrow$ *validator* $\Rightarrow$ *bool*
where
is-equivocating $\sigma\ v = (\exists\ m1 \in \sigma.\ \exists\ m2 \in \sigma.\ equivocation\ (m1,\ m2) \wedge sender\ m1 = v)$

definition *equivocating-validators* :: *state* $\Rightarrow$ *validator set*
where
equivocating-validators $\sigma = \{v \in observed\ \sigma.\ is\text{-}equivocating\ \sigma\ v\}$

lemma (**in** *Protocol*) *equivocating-validators-type* :
  $\forall\ \sigma \in \Sigma.$ *equivocating-validators* $\sigma \subseteq V$
  using *observed-type equivocating-validators-def* **by** *blast*

definition (**in** *Params*) *equivocating-validators-paper* :: *state* $\Rightarrow$ *validator set*
  where
    equivocating-validators-paper $\sigma = \{v \in V.$ *is-equivocating* $\sigma\ v\}$

lemma (**in** *Protocol*) *equivocating-validators-is-equivalent-to-paper* :
  $\forall\ \sigma \in \Sigma.$ *equivocating-validators* σ = *equivocating-validators-paper* σ
  by (*smt Collect-cong Params.equivocating-validators-paper-def equivocating-validators-def is-equivocating-def mem-Collect-eq observed-type observed-def subsetCE*)

definition (**in** *Params*) *equivocation-fault-weight* :: *state* $\Rightarrow$ *real*
  where
    equivocation-fault-weight σ = *sum* W (*equivocating-validators* σ)

definition (**in** *Params*) *is-faults-lt-threshold* :: *state* $\Rightarrow$ *bool*
  where
    is-faults-lt-threshold σ = (*equivocation-fault-weight* $\sigma < t$)

definition (**in** *Protocol*) Σt :: *state set*
  where
    $\Sigma t = \{\sigma \in \Sigma.$ *is-faults-lt-threshold* $\sigma\}$

lemma (**in** *Protocol*) *Σt-is-subset-of-Σ* : $\Sigma t \subseteq \Sigma$
  using *Σt-def* **by** *auto*

type-synonym *state-property* = *state* $\Rightarrow$ *bool*

type-synonym *consensus-value-property* = *consensus-value* $\Rightarrow$ *bool*

lemma (**in** *Protocol*) *transitivity-of-justifications* :
  transp-on justified M
  apply (*simp add*: *transp-on-def*)
  by (*meson Params.M-type Params.state-is-in-pow-M-i Protocol-axioms contra-subsetD justified-def*)

lemma (**in** *Protocol*) *irreflexivity-of-justifications* :
irreflp-on justified M
apply (*simp add*: *irreflp-on-def*)
apply (*simp add*: *justified-def*)
apply (*simp add*: *M-def*)
apply *auto*
proof −
fix *n m*
assume *est m* $\in$ *C*
assume *sender m* $\in$ *V*
assume *justification m* $\in$ Σ*-i* (V, C, ε) *n*
assume *est m* $\in$ ε (*justification m*)
assume *m* $\in$ *justification m*
have *m* $\in$ *M-i* (V, C, ε) ($n - 1$)
by (*smt M-i.simps One-nat-def Params.*Σ*i-subset-Mi Pow-iff Suc-pred* ‹*est m* $\in$ *C*› ‹*est m* $\in$ ε (*justification m*)› ‹*justification m* $\in$ Σ*-i* (V, C, ε) *n*› ‹*m* $\in$ *justification m*› ‹*sender m* $\in$ *V*› *add.right-neutral add-Suc-right diff-is-0-eq*′ *diff-le-self diff-zero mem-Collect-eq not-gr0 subsetCE*)
then have *justification m* $\in$ Σ*-i* (V, C, ε) ($n - 1$)
using *M-i.simps* **by** *blast*
then have *justification m* $\in$ Σ*-i* (V, C, ε) *0*
apply (*induction n*)
apply *simp*
by (*smt M-i.simps One-nat-def Params.*Σ*i-subset-Mi Pow-iff Suc-pred* ‹*m* $\in$ *justification m*› *add.right-neutral add-Suc-right diff-Suc-1 mem-Collect-eq not-gr0 subsetCE subsetCE*)
then have *justification m* $\in$ $\{\emptyset\}$
by *simp*
then show *False*
using ‹*m* $\in$ *justification m*› **by** *blast*
qed

lemma (**in** *Protocol*) *justification-is-strict-partial-order-on-M* :
po-on justified M
apply (*simp add*: *po-on-def*)
by (*simp add*: *irreflexivity-of-justifications transitivity-of-justifications*)

lemma (**in** *Protocol*) *monotonicity-of-justifications* :
$\forall$ *m m*′ σ. *m* $\in$ *M* $\wedge$ $\sigma \in \Sigma$ $\wedge$ *justified m*′ *m* $\longrightarrow$ *justification m*′ $\subseteq$ *justification m*
apply *simp*
by (*meson M-type justified-def message-in-state-is-valid state-is-in-pow-M-i*)

lemma (**in** *Protocol*) *strict-monotonicity-of-justifications* :
$\forall$ *m m*′ σ. *m* $\in$ *M* $\wedge$ $\sigma \in \Sigma$ $\wedge$ *justified m*′ *m* $\longrightarrow$ *justification m*′ $\subset$ *justification m*
by (*metis M-type irreflexivity-of-justifications irreflp-on-def justified-def message-in-state-is-valid monotonicity-of-justifications psubsetI*)

lemma (**in** *Protocol*) *justification-implies-different-messages* :
$\forall\ m\ m'.\ m \in M \wedge m' \in M \longrightarrow$ *justified* $m'\ m \longrightarrow m \neq m'$
by (*meson irreflexivity-of-justifications irreflp-on-def*)

lemma (**in** *Protocol*) *only-valid-message-is-justified* :
$\forall\ m \in M.\ \forall\ m'.$ *justified* $m'\ m \longrightarrow m' \in M$
apply (*simp add*: *justified-def*)
using *Params.M-type message-in-state-is-valid* **by** *blast*

lemma (**in** *Protocol*) *justified-message-exists-in-M-i-n-minus-1* :
$\forall\ n\ m\ m'.\ n \in \mathbb{N}$
$\longrightarrow$ *justified* $m'\ m$
$\longrightarrow m \in M\text{-}i\ (V,\ C,\ \varepsilon)\ n$
$\longrightarrow m' \in M\text{-}i\ (V,\ C,\ \varepsilon)\ (n - 1)$
proof −
have $\forall\ n\ m\ m'.$ *justified* $m'\ m$
$\longrightarrow m \in M\text{-}i\ (V,\ C,\ \varepsilon)\ n$
$\longrightarrow m \in M \wedge m' \in M$
$\longrightarrow m' \in M\text{-}i\ (V,\ C,\ \varepsilon)\ (n - 1)$
apply (*rule*, *rule*, *rule*, *rule*, *rule*, *rule*)
proof −
fix $n\ m\ m'$
assume *justified* $m'\ m$
assume $m \in M\text{-}i\ (V,\ C,\ \varepsilon)\ n$
assume $m \in M \wedge m' \in M$
then have *justification* $m \in \Sigma\text{-}i\ (V,C,\varepsilon)\ n$
using *M-i.simps* ‹$m \in M\text{-}i\ (V,\ C,\ \varepsilon)\ n$› **by** *blast*
then have *justification* $m \in$ *Pow* $(M\text{-}i\ (V,C,\varepsilon)\ (n - 1))$
by (*metis* (*no-types*, *lifting*) *Suc-diff-Suc* Σ*-i.simps*(*1*) Σ*i-subset-Mi* ‹*justified* $m'\ m$› *add-leE diff-add diff-le-self empty-iff justified-def neq0-conv plus-1-eq-Suc singletonD subsetCE*)
show $m' \in M\text{-}i\ (V,\ C,\ \varepsilon)\ (n - 1)$
using ‹*justification* $m \in$ *Pow* $(M\text{-}i\ (V,\ C,\ \varepsilon)\ (n - 1))$› ‹*justified* $m'\ m$› *justified-def* **by** *auto*
qed
then show *?thesis*
by (*metis* (*no-types*, *lifting*) *M-def UN-I only-valid-message-is-justified*)
qed

lemma (**in** *Protocol*) *monotonicity-of-card-of-justification* :
$\forall\ m\ m'.\ m \in M$
$\longrightarrow$ *justified* $m'\ m$
$\longrightarrow$ *card* (*justification* m') $<$ *card* (*justification* m)
by (*meson M-type Protocol.strict-monotonicity-of-justifications Protocol-axioms justification-is-finite psubset-card-mono*)

lemma (**in** *Protocol*) *justification-is-well-founded-on-M* :
wfp-on justified M
proof (*rule ccontr*)

assume ¬ *wfp-on justified M*
then have $\exists f.\ \forall i.\ f\ i \in M \wedge$ *justified* $(f\ (Suc\ i))\ (f\ i)$
by (*simp add*: *wfp-on-def*)
then obtain f **where** $\forall i.\ f\ i \in M \wedge$ *justified* $(f\ (Suc\ i))\ (f\ i)$ **by** *auto*
have $\forall\ i.$ *card* (*justification* $(f\ i)$) $\leq$ *card* (*justification* $(f\ 0)$) $-\ i$
apply (*rule*)
proof −
fix i
have *card* (*justification* $(f\ (Suc\ i))$) $<$ *card* (*justification* $(f\ i)$)
using ‹$\forall i.\ f\ i \in M \wedge$ *justified* $(f\ (Suc\ i))\ (f\ i)$› **by** (*simp add*: *monotonicity-of-card-of-justification*)
show *card* (*justification* $(f\ i)$) $\leq$ *card* (*justification* $(f\ 0)$) $-\ i$
apply (*induction* i)
apply *simp*
using ‹*card* (*justification* $(f\ (Suc\ i))$) $<$ *card* (*justification* $(f\ i)$)›
by (*smt Suc-diff-le* ‹$\forall i.\ f\ i \in M \wedge$ *justified* $(f\ (Suc\ i))\ (f\ i)$› *diff-Suc-Suc diff-is-0-eq le-iff-add less-Suc-eq-le less-imp-le monotonicity-of-card-of-justification not-less-eq-eq trans-less-add1*)
qed
then have $\exists\ i.\ i =$ *card* (*justification* $(f\ 0)$) $+\ Suc\ 0 \wedge$ *card* (*justification* $(f\ i)$) $\leq$ *card* (*justification* $(f\ 0)$) $-\ i$
by *blast*
then show *False*
using *le-0-eq le-simps*(*2*) *linorder-not-le monotonicity-of-card-of-justification nat-diff-split order-less-imp-le*
by (*metis* ‹$\forall i.\ f\ i \in M \wedge$ *justified* $(f\ (Suc\ i))\ (f\ i)$› *add.right-neutral add-Suc-right*)
qed

lemma (**in** *Protocol*) *subset-of-M-have-minimal-of-justification* :
$\forall\ S \subseteq M.\ S \neq \emptyset \longrightarrow (\exists\ m\text{-}min \in S.\ \forall\ m.$ *justified m m-min* $\longrightarrow m \notin S)$
by (*metis justification-is-well-founded-on-M wfp-on-imp-has-min-elt wfp-on-mono*)

end

2 Safety Proof

theory *ConsensusSafety*

imports *Main CBCCasper*

begin

fun (**in** *Protocol*) *futures* :: *state* ⇒ *state set*
where
futures $\sigma = \{\sigma' \in \Sigma t.$ *is-future-state* $(\sigma', \sigma)\}$

lemma (**in** *Protocol*) *monotonic-futures* :
$\forall\ \sigma'\ \sigma.\ \sigma' \in \Sigma t \wedge \sigma \in \Sigma t$
$\longrightarrow \sigma' \in \mathit{futures}\ \sigma \longleftrightarrow \mathit{futures}\ \sigma' \subseteq \mathit{futures}\ \sigma$
by *auto*

theorem (**in** *Protocol*) *two-party-common-futures* :
$\forall\ \sigma 1\ \sigma 2.\ \sigma 1 \in \Sigma t \wedge \sigma 2 \in \Sigma t$
$\longrightarrow (\sigma 1 \cup \sigma 2) \in \Sigma t$
$\longrightarrow \mathit{futures}\ \sigma 1 \cap \mathit{futures}\ \sigma 2 \neq \emptyset$
by *auto*

theorem (**in** *Protocol*) *n-party-common-futures* :
$\forall\ \sigma\text{-}set.\ \sigma\text{-}set \subseteq \Sigma t$
$\longrightarrow \bigcup\ \sigma\text{-}set \in \Sigma t$
$\longrightarrow \bigcap\ \{\mathit{futures}\ \sigma \mid \sigma.\ \sigma \in \sigma\text{-}set\} \neq \emptyset$
by *auto*

fun (**in** *Protocol*) *state-property-is-decided* :: (*state-property* $*$ *state*) $\Rightarrow$ *bool*
where
state-property-is-decided $(p, \sigma) = (\forall\ \sigma' \in \mathit{futures}\ \sigma\ .\ p\ \sigma')$

lemma (**in** *Protocol*) *forward-consistency* :
$\forall\ \sigma'\ \sigma.\ \sigma' \in \Sigma t \wedge \sigma \in \Sigma t$
$\longrightarrow \sigma' \in \mathit{futures}\ \sigma$
$\longrightarrow$ *state-property-is-decided* (p, σ)
$\longrightarrow$ *state-property-is-decided* (p, σ')
apply *simp*
by *auto*

fun *state-property-not* :: *state-property* $\Rightarrow$ *state-property*
where
state-property-not $p = (\lambda\sigma.\ (\neg\ p\ \sigma))$

lemma (**in** *Protocol*) *backword-consistency* :
$\forall\ \sigma'\ \sigma.\ \sigma' \in \Sigma t \wedge \sigma \in \Sigma t$
$\longrightarrow \sigma' \in \mathit{futures}\ \sigma$
$\longrightarrow$ *state-property-is-decided* (p, σ')
$\longrightarrow \neg$*state-property-is-decided* (*state-property-not* p, σ)
apply *simp*
by *auto*

theorem (**in** *Protocol*) *two-party-consensus-safety* :
$\forall\ \sigma 1\ \sigma 2.\ \sigma 1 \in \Sigma t \wedge \sigma 2 \in \Sigma t$
$\longrightarrow (\sigma 1 \cup \sigma 2) \in \Sigma t$
$\longrightarrow \neg($*state-property-is-decided* $(p, \sigma 1) \wedge$ *state-property-is-decided* $($*state-property-not* $p, \sigma 2))$
by *auto*

fun (**in** *Protocol*) *state-properties-are-inconsistent* :: *state-property set* $\Rightarrow$ *bool*
where
state-properties-are-inconsistent p-set $= (\forall\ \sigma \in \Sigma.\ \neg\ (\forall\ p \in$ *p-set*$.\ p\ \sigma))$

fun (**in** *Protocol*) *state-properties-are-consistent* :: *state-property set* $\Rightarrow$ *bool*
where
state-properties-are-consistent p-set $= (\exists\ \sigma \in \Sigma.\ \forall\ p \in$ *p-set*$.\ p\ \sigma)$

fun (**in** *Protocol*) *state-property-decisions* :: *state* $\Rightarrow$ *state-property set*
where
state-property-decisions $\sigma = \{p.$ *state-property-is-decided* $(p, \sigma)\}$

theorem (**in** *Protocol*) *n-party-safety-for-state-properties* :
$\forall$ σ*-set*. σ*-set* $\subseteq \Sigma t$
$\longrightarrow \bigcup$ σ*-set* $\in \Sigma t$
$\longrightarrow$ *state-properties-are-consistent* $(\bigcup\ \{$*state-property-decisions* $\sigma \mid \sigma.\ \sigma \in \sigma$*-set*$\})$
apply *rule+*
proof−
fix σ*-set*
assume σ*-set*: σ*-set* $\subseteq \Sigma t$

assume $\bigcup$ σ*-set* $\in \Sigma t$
hence $\bigcap\ \{$*futures* $\sigma \mid \sigma.\ \sigma \in \sigma$*-set*$\} \neq \emptyset$
using σ*-set* **by** *auto*
hence $\exists\sigma{\in}\Sigma t.\ \sigma \in \bigcap\ \{$*futures* $\sigma \mid \sigma.\ \sigma \in \sigma$*-set*$\}$
using $\langle\bigcup\sigma$*-set* $\in \Sigma t\rangle$ **by** *fastforce*
hence $\exists\sigma{\in}\Sigma t.\ \forall s{\in}\sigma$*-set*$.\ \sigma \in$ *futures s*
by *blast*
hence $\exists\sigma{\in}\Sigma t.\ (\forall s{\in}\sigma$*-set*$.\ \sigma \in$ *futures s*$) \wedge (\forall s{\in}\sigma$*-set*$.\ \sigma \in$ *futures s* $\longrightarrow (\forall p.$ *state-property-is-decided* $(p,s) \longrightarrow$ *state-property-is-decided* $(p,\sigma)))$
by (*simp add*: *subset-eq*)
hence $\exists\sigma{\in}\Sigma t.\ \forall s{\in}\sigma$*-set*$.\ (\forall p.$ *state-property-is-decided* $(p,s) \longrightarrow$ *state-property-is-decided* $(p,\sigma))$
by *blast*
hence $\exists\sigma{\in}\Sigma t.\ \forall s{\in}\sigma$*-set*$.\ (\forall p \in$ *state-property-decisions s*. *state-property-is-decided* $(p,\sigma))$

by *simp*
hence $\exists\,\sigma\in\Sigma t.\ \forall\,p\in\bigcup\{$*state-property-decisions* $\sigma \mid \sigma.\ \sigma \in \sigma$*-set*$\}$. *state-property-is-decided* (p,σ)
proof−
obtain σ **where** $\sigma \in \Sigma t\ \forall\, s\in\sigma$*-set*. $(\forall\, p \in$ *state-property-decisions s*. *state-property-is-decided* $(p,\sigma))$
using ‹$\exists\,\sigma\in\Sigma t.\ \forall\, s\in\sigma$*-set*. $\forall\, p\in$*state-property-decisions s*. *state-property-is-decided* $(p,\ \sigma)$› **by** *blast*
have $\forall\, p\in\bigcup\{$*state-property-decisions* $\sigma \mid \sigma.\ \sigma \in \sigma$*-set*$\}$. *state-property-is-decided* (p,σ)
using ‹$\forall\, s\in\sigma$*-set*. $\forall\, p\in$*state-property-decisions s*. *state-property-is-decided* $(p,\ \sigma)$› **by** *fastforce*
thus *?thesis*
using ‹$\sigma \in \Sigma t$› **by** *blast*
qed
hence $\exists\,\sigma\in\Sigma t.\ \forall\, p\in\bigcup\{$*state-property-decisions* $\sigma \mid \sigma.\ \sigma \in \sigma$*-set*$\}$. $\forall\,\sigma'\in$*futures* $\sigma.\ p\ \sigma'$
by *simp*
show *state-properties-are-consistent* $(\bigcup\{$*state-property-decisions* $\sigma \mid \sigma.\ \sigma \in \sigma$*-set*$\})$
by (*metis* (*mono-tags*, *lifting*) Σt*-def* ‹$\exists\,\sigma\in\Sigma t.\ \forall\, p\in\bigcup\{$*state-property-decisions* $\sigma \mid \sigma.\ \sigma \in \sigma$*-set*$\}$. $\forall\,\sigma'\in$*futures* $\sigma.\ p\ \sigma'$› *mem-Collect-eq monotonic-futures order-refl state-properties-are-consistent.simps*)
qed

fun (**in** *Protocol*) *naturally-corresponding-state-property* :: *consensus-value-property* $\Rightarrow$ *state-property*
where
naturally-corresponding-state-property $q = (\lambda\sigma.\ \forall\ c \in \varepsilon\ \sigma.\ q\ c)$

fun (**in** *Protocol*) *consensus-value-properties-are-consistent* :: *consensus-value-property set* $\Rightarrow$ *bool*
where
consensus-value-properties-are-consistent q-set $= (\exists\ c \in C.\ \forall\ q \in$ *q-set*. $q\ c)$

lemma (**in** *Protocol*) *naturally-corresponding-consistency* :
$\forall$ *q-set*. *state-properties-are-consistent* $\{$*naturally-corresponding-state-property q* $\mid q.\ q \in$ *q-set*$\}$
$\longrightarrow$ *consensus-value-properties-are-consistent q-set*
apply (*rule*, *rule*)
proof −
fix *q-set*

have
state-properties-are-consistent $\{$*naturally-corresponding-state-property q* $\mid q.\ q$

$\in$ *q-set*}
$\longrightarrow (\exists\ \sigma \in \Sigma.\ \forall\ p \in \{\lambda\sigma'.\ \forall\ c \in \varepsilon\ \sigma'.\ q\ c \mid q.\ q \in \textit{q-set}\}.\ p\ \sigma)$
by *simp*
moreover have
$(\exists\ \sigma \in \Sigma.\ \forall\ p \in \{\lambda\sigma'.\ \forall\ c \in \varepsilon\ \sigma'.\ q\ c \mid q.\ q \in \textit{q-set}\}.\ p\ \sigma)$
$\longrightarrow (\exists\ \sigma \in \Sigma.\ \forall\ q' \in \textit{q-set}.\ (\lambda\sigma'.\ \forall\ c \in \varepsilon\ \sigma'.\ q'\ c)\ \sigma)$
by (*metis* (*mono-tags*, *lifting*) *mem-Collect-eq*)
moreover have
$(\exists\ \sigma \in \Sigma.\ \forall\ q \in \textit{q-set}.\ (\lambda\sigma'.\ \forall\ c \in \varepsilon\ \sigma'.\ q\ c)\ \sigma)$
$\longrightarrow (\exists\ \sigma \in \Sigma.\ \forall\ q' \in \textit{q-set}.\ \forall\ c \in \varepsilon\ \sigma.\ q'\ c)$
by *blast*
moreover have
$(\exists\ \sigma \in \Sigma.\ \forall\ q \in \textit{q-set}.\ \forall\ c \in \varepsilon\ \sigma.\ q\ c)$
$\longrightarrow (\exists\ \sigma \in \Sigma.\ \forall\ c \in \varepsilon\ \sigma.\ \forall\ q' \in \textit{q-set}.\ q'\ c)$
by *blast*
moreover have
$(\exists\ \sigma \in \Sigma.\ \forall\ c \in \varepsilon\ \sigma.\ \forall\ q \in \textit{q-set}.\ q\ c)$
$\longrightarrow (\exists\ \sigma \in \Sigma.\ \exists\ c \in \varepsilon\ \sigma.\ \forall\ q' \in \textit{q-set}.\ q'\ c)$
by (*meson all-not-in-conv estimates-are-non-empty*)
moreover have
$(\exists\ \sigma \in \Sigma.\ \exists\ c \in \varepsilon\ \sigma.\ \forall\ q \in \textit{q-set}.\ q\ c)$
$\longrightarrow (\exists\ c \in C.\ \forall\ q' \in \textit{q-set}.\ q'\ c)$
using *is-valid-estimator-def* ε*-type* **by** *fastforce*
ultimately show
state-properties-are-consistent {*naturally-corresponding-state-property q* |*q*. *q* $\in$ *q-set*}
$\Longrightarrow$ *consensus-value-properties-are-consistent q-set*
by *simp*
qed

fun (**in** *Protocol*) *consensus-value-property-is-decided* :: (*consensus-value-property* $*$ *state*) $\Rightarrow$ *bool*
where
consensus-value-property-is-decided (q, σ)
= *state-property-is-decided* (*naturally-corresponding-state-property* q, σ)

fun (**in** *Protocol*) *consensus-value-property-decisions* :: *state* $\Rightarrow$ *consensus-value-property set*
where
consensus-value-property-decisions σ = {q. *consensus-value-property-is-decided* (q, σ)}

theorem (**in** *Protocol*) *n-party-safety-for-consensus-value-properties* :
$\forall\ \sigma\textit{-set}.\ \sigma\textit{-set} \subseteq \Sigma t$
$\longrightarrow \bigcup\ \sigma\textit{-set} \in \Sigma t$
$\longrightarrow$ *consensus-value-properties-are-consistent* ($\bigcup$ {*consensus-value-property-decisions*

$\sigma \mid \sigma.\ \sigma \in \sigma\text{-}set\})$
  apply (*rule*, *rule*, *rule*)
proof −
  fix σ-*set*
  assume $\sigma\text{-}set \subseteq \Sigma t$

  assume $\bigcup\ \sigma\text{-}set \in \Sigma t$
  hence *state-properties-are-consistent* $(\bigcup\ \{state\text{-}property\text{-}decisions\ \sigma \mid \sigma.\ \sigma \in \sigma\text{-}set\})$
    using ‹$\sigma\text{-}set \subseteq \Sigma t$› *n-party-safety-for-state-properties* **by** *auto*
  hence *state-properties-are-consistent* $\{p \in \bigcup\ \{state\text{-}property\text{-}decisions\ \sigma \mid \sigma.\ \sigma \in \sigma\text{-}set\}.\ \exists\ q.\ p = naturally\text{-}corresponding\text{-}state\text{-}property\ q\}$
    apply *simp*
    by *meson*
  hence *state-properties-are-consistent* $\{naturally\text{-}corresponding\text{-}state\text{-}property\ q \mid q.\ naturally\text{-}corresponding\text{-}state\text{-}property\ q \in \bigcup\ \{state\text{-}property\text{-}decisions\ \sigma \mid \sigma.\ \sigma \in \sigma\text{-}set\}\}$
    by (*smt Collect-cong*)
  hence *consensus-value-properties-are-consistent* $\{q.\ naturally\text{-}corresponding\text{-}state\text{-}property\ q \in \bigcup\ \{state\text{-}property\text{-}decisions\ \sigma \mid \sigma.\ \sigma \in \sigma\text{-}set\}\}$
    using *naturally-corresponding-consistency*
  proof −
    show *?thesis*
     by (*metis* (*no-types*) *Setcompr-eq-image* ‹$\forall\ q\text{-}set.\ state\text{-}properties\text{-}are\text{-}consistent\ \{naturally\text{-}corresponding\text{-}state\text{-}property\ q \mid q.\ q \in q\text{-}set\} \longrightarrow consensus\text{-}value\text{-}properties\text{-}are\text{-}consistent\ q\text{-}set$› ‹$state\text{-}properties\text{-}are\text{-}consistent\ \{naturally\text{-}corresponding\text{-}state\text{-}property\ q \mid q.\ naturally\text{-}corresponding\text{-}state\text{-}property\ q \in \bigcup\{state\text{-}property\text{-}decisions\ \sigma \mid \sigma.\ \sigma \in \sigma\text{-}set\}\}$› *setcompr-eq-image*)
  qed
  hence *consensus-value-properties-are-consistent* $(\bigcup\ \{consensus\text{-}value\text{-}property\text{-}decisions\ \sigma \mid \sigma.\ \sigma \in \sigma\text{-}set\})$
    apply *simp*
    by (*smt mem-Collect-eq*)
  thus
   consensus-value-properties-are-consistent $(\bigcup\ \{consensus\text{-}value\text{-}property\text{-}decisions\ \sigma \mid \sigma.\ \sigma \in \sigma\text{-}set\})$
    by *simp*
qed

end

3 Latest Message

theory *LatestMessage*

imports *Main CBCCasper*

begin

definition *later* :: (*message* ∗ *state*) ⇒ *message set*
  where
    later = (λ(*m*, σ). {*m*′ ∈ σ. *justified m m*′})

lemma (**in** *Protocol*) *later-type* :
  ∀ σ *m*. $\sigma \in \Sigma \wedge m \in M \longrightarrow$ *later* (*m*, σ) ⊆ *M*
  apply (*simp add*: *later-def*)
  using *state-is-subset-of-M* **by** *auto*

definition *from-sender* :: (*validator* ∗ *state*) ⇒ *message set*
  where
    from-sender = (λ(*v*, σ). {*m* ∈ σ. *sender m* = *v*})

lemma (**in** *Protocol*) *from-sender-type* :
  ∀ σ *v*. $\sigma \in \Sigma \wedge v \in V \longrightarrow$ *from-sender* (*v*, σ) ⊆ *M*
  apply (*simp add*: *from-sender-def*)
  using *state-is-subset-of-M* **by** *auto*

definition *from-group* :: (*validator set* ∗ *state*) ⇒ *state*
  where
    from-group = (λ(*v-set*, σ). {*m* ∈ σ. *sender m* ∈ *v-set*})

lemma (**in** *Protocol*) *from-group-type* :
  ∀ σ *v*. $\sigma \in \Sigma \wedge$ *v-set* ⊆ *V* ⟶ *from-group* (*v-set*, σ) ⊆ *M*
  apply (*simp add*: *from-group-def*)
  using *state-is-subset-of-M* **by** *auto*

definition *later-from* :: (*message* ∗ *validator* ∗ *state*) ⇒ *message set*
  where
    later-from = (λ(*m*, *v*, σ). *later* (*m*, σ) ∩ *from-sender* (*v*, σ))

lemma (**in** *Protocol*) *later-from-type* :
  ∀ σ *v m*. $\sigma \in \Sigma \wedge v \in V \wedge m \in M \longrightarrow$ *later-from* (*m*, *v*, σ) ⊆ *M*
  apply (*simp add*: *later-from-def*)
  using *later-type from-sender-type* **by** *auto*

definition *latest-messages* :: *state* ⇒ (*validator* ⇒ *state*)
  where

$latest\text{-}messages\ \sigma\ v = \{m \in from\text{-}sender\ (v, \sigma).\ later\text{-}from\ (m, v, \sigma) = \emptyset\}$

lemma (**in** *Protocol*) *latest-messages-type* :
$\forall\ \sigma\ v.\ \sigma \in \Sigma \wedge v \in V \longrightarrow latest\text{-}messages\ \sigma\ v \subseteq M$
apply (*simp add*: *latest-messages-def later-from-def*)
using *from-sender-type* **by** *auto*

lemma (**in** *Protocol*) *latest-messages-from-non-observed-validator-is-empty* :
$\forall\ \sigma\ v.\ \sigma \in \Sigma \wedge v \in V \wedge v \notin observed\ \sigma \longrightarrow latest\text{-}messages\ \sigma\ v = \emptyset$
by (*simp add*: *latest-messages-def observed-def later-def from-sender-def*)

definition *latest-estimates* :: *state* ⇒ *validator* ⇒ *consensus-value set*
where
$latest\text{-}estimates\ \sigma\ v = \{est\ m \mid m.\ m \in latest\text{-}messages\ \sigma\ v\}$

lemma (**in** *Protocol*) *latest-estimates-type* :
$\forall\ \sigma\ v.\ \sigma \in \Sigma \wedge v \in V \longrightarrow latest\text{-}estimates\ \sigma\ v \subseteq C$
using *M-type Protocol.latest-messages-type Protocol-axioms latest-estimates-def*
by *fastforce*

lemma (**in** *Protocol*) *latest-estimates-from-non-observed-validator-is-empty* :
$\forall\ \sigma\ v.\ \sigma \in \Sigma \wedge v \in V \wedge v \notin observed\ \sigma \longrightarrow latest\text{-}estimates\ \sigma\ v = \emptyset$
using *latest-estimates-def latest-messages-from-non-observed-validator-is-empty*
by *auto*

fun *observed-non-equivocating-validators* :: *state* ⇒ *validator set*
where
$observed\text{-}non\text{-}equivocating\text{-}validators\ \sigma = observed\ \sigma - equivocating\text{-}validators\ \sigma$

lemma (**in** *Protocol*) *observed-non-equivocating-validators-type* :
$\forall\ \sigma \in \Sigma.\ observed\text{-}non\text{-}equivocating\text{-}validators\ \sigma \subseteq V$
using *observed-type equivocating-validators-type* **by** *auto*

lemma (**in** *Protocol*) *justification-is-well-founded-on-messages-from-validator*:
$\forall\ \sigma \in \Sigma.\ (\forall\ v \in V.\ \ wfp\text{-}on\ justified\ (from\text{-}sender\ (v, \sigma)))$
using *justification-is-well-founded-on-M from-sender-type wfp-on-subset* **by** *blast*

lemma (**in** *Protocol*) *justification-is-strict-partial-order-on-messages-from-validator*:
$\forall\ \sigma \in \Sigma.\ (\forall\ v \in V.\ \ po\text{-}on\ justified\ (from\text{-}sender\ (v, \sigma)))$

using *justification-is-strict-partial-order-on-M from-sender-type po-on-subset* **by** *blast*

definition *strict-linear-order-on* :: $('a \Rightarrow 'a \Rightarrow bool) \Rightarrow 'a\ set \Rightarrow bool$
where
strict-linear-order-on $P\ A \equiv$ *po-on* $P\ A\ \wedge$ *total-on* $P\ A$

definition *strict-well-order-on* :: $('a \Rightarrow 'a \Rightarrow bool) \Rightarrow 'a\ set \Rightarrow bool$
where
strict-well-order-on $P\ A \equiv$ *strict-linear-order-on* $P\ A\ \wedge$ *wfp-on* $P\ A$

lemma (**in** *Protocol*) *justification-is-total-on-messages-from-non-equivocating-validator*:
$\forall\ \sigma \in \Sigma.\ (\forall\ v \in V.\ v \notin$ *equivocating-validators* $\sigma \longrightarrow$ *total-on justified* (*from-sender* $(v, \sigma)))$
proof −
have $\forall\ m1\ m2\ \sigma\ v.\ v \in V \wedge \sigma \in \Sigma \wedge \{m1, m2\} \subseteq$ *from-sender* $(v, \sigma) \longrightarrow$ *sender* $m1 =$ *sender* $m2$
by (*simp add*: *from-sender-def*)
then have $\forall\ \sigma \in \Sigma.\ (\forall\ v \in V.\ v \notin$ *equivocating-validators* σ
$\longrightarrow (\forall\ m1\ m2.\ \{m1, m2\} \subseteq$ *from-sender* $(v, \sigma) \longrightarrow m1 = m2 \vee$ *justified* $m1\ m2 \vee$ *justified* $m2\ m1))$
apply (*simp add*: *equivocating-validators-def is-equivocating-def equivocation-def from-sender-def observed-def*)
by *blast*
then show *?thesis*
by (*simp add*: *total-on-def*)
qed

lemma (**in** *Protocol*) *justification-is-strict-well-order-on-messages-from-non-equivocating-validator*:
$\forall\ \sigma \in \Sigma.\ (\forall\ v \in V.\ v \notin$ *equivocating-validators* $\sigma \longrightarrow$ *strict-well-order-on justified* (*from-sender* $(v, \sigma)))$
apply (*simp add*: *strict-well-order-on-def strict-linear-order-on-def*)
using *justification-is-total-on-messages-from-non-equivocating-validator*
justification-is-well-founded-on-messages-from-validator
justification-is-strict-partial-order-on-messages-from-validator
by *auto*

lemma (**in** *Protocol*) *observed-non-equivocating-validators-have-one-latest-message*:
$\forall\ \sigma \in \Sigma.\ (\forall\ v \in$ *observed-non-equivocating-validators* $\sigma.$ *card* (*latest-message* $\sigma\ v) = 1)$
oops

lemma (**in** *Protocol*) *non-equivocating-validators-have-at-most-one-latest-message*:
$\forall\ \sigma \in \Sigma.\ (\forall\ v \in V.\ v \notin$ *equivocating-validators* $\sigma \longrightarrow$ *card* (*latest-message* $\sigma\ v)$

$\leq$ *1*)
oops

lemma (**in** *Protocol*) *monotonicity-of-justifications* :
$\forall\ m\ m'\ \sigma.\ m \in M \wedge \sigma \in \Sigma \wedge m' \in$ *later* $(m, \sigma) \longrightarrow$ *justification* $m \subseteq$ *justification* m'
apply (*simp add*: *later-def*)
by (*meson M-type justified-def message-in-state-is-valid state-is-in-pow-M-i*)

definition *latest-messages-from-non-equivocating-validators* :: *state* $\Rightarrow$ *validator* $\Rightarrow$ *message set*
where
latest-messages-from-non-equivocating-validators σ v = (*if is-equivocating* σ v *then* $\emptyset$ *else latest-messages* σ v)

lemma (**in** *Protocol*) *latest-messages-from-non-equivocating-validators-type* :
$\forall\ \sigma\ v.\ \sigma \in \Sigma \wedge v \in V \longrightarrow$ *latest-messages-from-non-equivocating-validators* σ v $\subseteq M$
by (*simp add*: *latest-messages-type latest-messages-from-non-equivocating-validators-def*)

definition *latest-estimates-from-non-equivocating-validators* :: *state* $\Rightarrow$ *validator* $\Rightarrow$ *consensus-value set*
where
latest-estimates-from-non-equivocating-validators σ v = {*est* m | m. $m \in$ *latest-messages-from-non-equivocating-validators* σ v}

lemma (**in** *Protocol*) *latest-estimates-from-non-equivocating-validators-type* :
$\forall\ \sigma\ v.\ \sigma \in \Sigma \wedge v \in V \longrightarrow$ *latest-estimates-from-non-equivocating-validators* σ v $\subseteq C$
using *Protocol.latest-estimates-type Protocol-axioms latest-estimates-def latest-estimates-from-non-equivocati*
latest-messages-from-non-equivocating-validators-def **by** *auto*

lemma (**in** *Protocol*) *latest-estimates-from-non-equivocating-validators-from-non-observed-validator-is-empty* :
$\forall\ \sigma\ v.\ \sigma \in \Sigma \wedge v \in V \wedge v \notin$ *observed* $\sigma \longrightarrow$ *latest-estimates-from-non-equivocating-validators* σ $v = \emptyset$
by (*simp add*: *latest-estimates-from-non-equivocating-validators-def latest-messages-from-non-equivocating-va*

latest-messages-from-non-observed-validator-is-empty)

end