Formalization of a Generalized Protocol for Clock Synchronization in Isabelle/HOL

Alwen Tiu

January 9, 2020

Abstract

We formalize the generalized Byzantine fault-tolerant clock synchronization protocol of Schneider. This protocol abstracts from particular algorithms or implementations for clock synchronization. This abstraction includes several assumptions on the behaviors of physical clocks and on general properties of concrete algorithms/implementations. Based on these assumptions the correctness of the protocol is proved by Schneider. His proof was later verified by Shankar using the theorem prover EHDM (precursor to PVS). Our formalization in Isabelle/HOL is based on Shankar’s formalization.

Contents

1 Introduction ......................................................... 1

2 Isar proof scripts .................................................... 2

2.1 Types and constants definitions ................................. 2

2.2 Clock conditions .................................................. 3

2.2.1 Some derived properties of clocks ......................... 5

2.2.2 Bounded-drift for logical clocks (IC) ...................... 6

2.3 Agreement property .............................................. 10

1 Introduction

In certain distributed systems, e.g., real-time process-control systems, the existence of a reliable global time source is critical in ensuring the correct functioning of the systems. This reliable global time source can be implemented using several physical clocks distributed on different nodes in the distributed system. Since physical clocks are by nature constantly drifting away from the “real time” and different clocks can have different drift rates, in such a scheme, it is important that these clocks are regularly adjusted so that they are closely synchronized within a certain application-specific safe bound. The design and verification of clock synchronization protocols are often complicated by the additional requirement that the protocols should work correctly under certain types of errors, e.g., failure of some clocks, error in communication network or corrupted messages, etc.

There has been a number of fault-tolerant clock synchronization algorithms studied in the literature, e.g., the Interactive Convergence Algorithm (ICA) by Lamport and Melliar-Smith [1], the Lundelius-Lynch algorithm [2], etc., each with its own degree of fault tolerance. One important property that
must be satisfied by a clock synchronization algorithm is the agreement property, i.e., at any time $t$, the difference of the clock readings of any two non-faulty processes must be bounded by a constant (which is fixed according to the domain of applications). At the core of these algorithms is the convergence function that calculates the adjustment to a clock of a process, based on the clock readings of all other processes. Schneider [3] gives an abstract characterization of a wide range of clock synchronization algorithms (based on the convergence functions used) and proves the agreement property in this abstract framework. Schneider’s proof was later verified by Shankar [4] in the theorem prover EHDM (precursor to PVS), where eleven axioms about clocks are explicitly stated.

We formalize Schneider’s proof in Isabelle/HOL, making use of Shankar’s formulation of the clock axioms. The particular formulation of axioms on clock conditions and the statements of the main theorems here are essentially those of Shankar’s [4], with some minor changes in syntax. For the full description of the protocol, the general structure of the proof and the meaning of the constants and function symbols used in this formalization, we refer readers to [4].

Acknowledgment  I would like to thank Stephan Merz and Pascal Fontaine for useful tips on using Isabelle and particularly the Isar proof language.

2  Isar proof scripts

theory GenClock imports Complex-Main begin

2.1 Types and constants definitions

Process is represented by natural numbers. The type ’event’ corresponds to synchronization rounds.

`type-synonym process = nat`

`type-synonym event = nat`

`type-synonym time = real`

`type-synonym Clocktime = real`

axiomatization

`δ :: real and`

`µ :: real and`

`ϱ :: real and`

`rmin :: real and`

`rmax :: real and`

`β :: real and`

`Λ :: real and`

`np :: process and`

`maxfaults :: process and`

`PC :: [process, time] ⇒ Clocktime and`

`VC :: [process, time] ⇒ Clocktime and`

`te :: [process, event] ⇒ time and`
\vartheta :: \text{process, event} \Rightarrow \text{process} \Rightarrow \text{Clocktime} \text{ and}

\text{IC} :: \text{process, event, time} \Rightarrow \text{Clocktime} \text{ and}

correct :: \text{process, time} \Rightarrow \text{bool} \text{ and}

cfn :: \text{process, (process } \Rightarrow \text{Clocktime)}] \Rightarrow \text{Clocktime} \text{ and}

\pi :: \text{Clocktime, Clocktime} \Rightarrow \text{Clocktime} \text{ and}

\alpha :: \text{Clocktime} \Rightarrow \text{Clocktime}

definition

count :: \text{process } \Rightarrow \text{bool, process} \Rightarrow \text{nat} \text{ where}
count f n = \text{card} \left\{ p. \ p < n \land f p \right\}

definition

\text{Adj} :: \text{process, event} \Rightarrow \text{Clocktime} \text{ where}
\text{Adj} = (\lambda p i. \text{ if } 0 < i \text{ then } \text{cfn} p (\vartheta p i) - \text{PC} p (\text{te} p i)
\text{ else } 0)

definition

\text{okRead1} :: \text{process } \Rightarrow \text{Clocktime, Clocktime, process } \Rightarrow \text{bool} \Rightarrow \text{bool} \text{ where}
\text{okRead1} f x \text{ppred} \longleftrightarrow (\forall l m. \text{ppred} l \land \text{ppred} m \longrightarrow |f l - f m| \leq x)

definition

\text{okRead2} :: \text{process } \Rightarrow \text{Clocktime, process } \Rightarrow \text{Clocktime, Clocktime, Clocktime, process } \Rightarrow \text{bool} \Rightarrow \text{bool} \text{ where}
\text{okRead2} f g x \text{ppred} \longleftrightarrow (\forall p. \text{ppred} p \longrightarrow |f p - g p| \leq x)

definition

\text{rho-bound1} :: [[\text{process, time} \Rightarrow \text{Clocktime} \Rightarrow \text{bool} \text{ where}
\text{rho-bound1} C \longleftrightarrow (\forall p s t. \text{correct} p t \land s \leq t \longrightarrow \text{C} p t - \text{C} p s \leq (t - s)* (1 + \rho))

definition

\text{rho-bound2} :: [[\text{process, time} \Rightarrow \text{Clocktime} \Rightarrow \text{bool} \text{ where}
\text{rho-bound2} C \longleftrightarrow (\forall p s t. \text{correct} p t \land s \leq t \longrightarrow (t - s)* (1 - \rho) \leq C p t - C p s)

2.2 Clock conditions

Some general assumptions

axiomatization where

\text{constants-ax: } 0 < \beta \land 0 < \mu \land 0 < rmin
\land rmin \leq rmax \land 0 < \rho \land 0 < np \land \text{maxfaults} \leq np

axiomatization where

\text{PC-monotone: } \forall p s t. \text{correct} p t \land s \leq t \longrightarrow \text{PC} p s \leq \text{PC} p t

axiomatization where

\text{VClock: } \forall p t i. \text{correct} p t \land \text{te} p i \leq t \land t < \text{te} p (i + 1) \longrightarrow \text{VC} p t = \text{IC} p i t
axiomatization where
\[ I_{\text{Clock}}: \forall p t i. \text{correct } p t \rightarrow I_C p i t = PC p t + \text{Adj } p i \]

Condition 1: initial skew
\[ \text{init: } \forall p. \text{correct } p 0 \rightarrow 0 \leq PC p 0 \land PC p 0 \leq \mu \]

Condition 2: bounded drift
axiomatization where
\[ \text{rate-1: } \forall p s t. \text{correct } p t \land s \leq t \rightarrow PC p t - PC p s \leq (t - s) \cdot (t + g) \text{ and} \]
\[ \text{rate-2: } \forall p s t. \text{correct } p t \land s \leq t \rightarrow (t - s) \cdot (1 - g) \leq PC p t - PC p s \]

Condition 3: bounded interval
axiomatization where
\[ \text{rts0: } \forall p t i. \text{correct } p t \land t \leq te p (i+1) \rightarrow t - te p i \leq r_{\text{max}} \text{ and} \]
\[ \text{rts1: } \forall p t i. \text{correct } p t \land te p (i+1) \leq t \rightarrow r_{\text{min}} \leq t - te p i \]

Condition 4: bounded delay
axiomatization where
\[ \text{rts2a: } \forall p q i. \text{correct } p t \land \text{correct } q t \land te q i + \beta \leq t \rightarrow te p i \leq t \text{ and} \]
\[ \text{rts2b: } \forall p q i. \text{correct } p (te p i) \land \text{correct } q (te q i) \rightarrow abs(te p i - te q i) \leq \beta \]

Condition 5: initial synchronization
axiomatization where
\[ \text{synch0: } \forall p. \text{te } p 0 = 0 \]

Condition 6: nonoverlap
axiomatization where
\[ \text{nonoverlap: } \beta \leq r_{\text{min}} \]

Condition 7: reading errors
axiomatization where
\[ \text{readerror: } \forall p q i. \text{correct } p (te p (i+1)) \land \text{correct } q (te p (i+1)) \rightarrow \]
\[ \text{abs}(\vartheta p (i+1) q - I_C q i (te p (i+1))) \leq \Lambda \]

Condition 8: bounded faults
axiomatization where
\[ \text{correct-closed: } \forall p s t. s \leq t \land \text{correct } p t \rightarrow \text{correct } p s \text{ and} \]
\[ \text{correct-count: } \forall t. np - \text{maxfaults } \leq \text{count } (\lambda p. \text{correct } p t) np \]

Condition 9: Translation invariance
axiomatization where
\[ \text{trans-inv: } \forall p f x. 0 \leq x \rightarrow cfn p (\lambda y. f y + x) = cfn p f + x \]

Condition 10: precision enhancement
axiomatization where
\[ \text{prec-eh: }\]
\[ \forall ppred p q f g x y.\]
\[ np - \text{maxfaults } \leq \text{count } ppred np \land \]
\[ \text{okRead1 } f y ppred \land \text{okRead1 } g y ppred \land \]

4
\[ \text{okRead}2 \ f \ g \ x \ \text{ppred} \land \text{ppred} \ p \land \text{ppred} \ q \rightarrow \text{abs}(\text{cfn}\ p\ f - \text{cfn}\ q\ g) \leq \pi\ x\ y \]

Condition 11: accuracy preservation

axiomatization where

\[ \forall \ \text{ppred} \ p \ q \ f \ x. \ \text{okRead}1 \ f \ x \ \text{ppred} \land \text{ppred} \ p \land \text{ppred} \ q \rightarrow \text{abs}(\text{cfn}\ p\ f - \text{cfn}\ q\ g) \leq \alpha\ x\ y \]

2.2.1 Some derived properties of clocks

lemma rts0d:
assumes \( cp: \text{correct} \ p \ (\text{te}\ p\ (i+1)) \)
shows \( \text{te}\ p\ (i+1) - \text{te}\ p\ i \leq \text{rmax} \)
using \( cp \) rts0 by simp

lemma rts1d:
assumes \( cp: \text{correct} \ p \ (\text{te}\ p\ (i+1)) \)
shows \( \text{rmin} \leq \text{te}\ p\ (i+1) - \text{te}\ p\ i \)
using \( cp \) rts1 by simp

lemma rte:
assumes \( cp: \text{correct} \ p \ (\text{te}\ p\ (i+1)) \)
shows \( \text{te}\ p\ i \leq \text{te}\ p\ (i+1) \)
proof –
from \( cp \) rts1d have \( \text{rmin} \leq \text{te}\ p\ (i+1) - \text{te}\ p\ i \)
by simp
from this \( \text{constants-ax} \) show \( \text{thesis} \) by arith
qed

lemma beta-bound1:
assumes \( \text{corr-p}: \text{correct} \ p \ (\text{te}\ p\ (i+1)) \)
and \( \text{corr-q}: \text{correct} \ q \ (\text{te}\ p\ (i+1)) \)
shows \( 0 \leq \text{te}\ p\ (i+1) - \text{te}\ q\ i \)
proof –
from \( \text{corr-p} \) rte have \( \text{te}\ p\ i \leq \text{te}\ p\ (i+1) \)
by simp
from this \( \text{corr-p correct-closed} \) have \( \text{corr-pi}: \text{correct} \ p \ (\text{te}\ p\ i) \)
by blast
from \( \text{corr-p} \) rts1d nonoverlap have \( \text{rmin} \leq \text{te}\ p\ (i+1) - \text{te}\ p\ i \)
by simp
from this nonoverlap have \( \beta \leq \text{te}\ p\ (i+1) - \text{te}\ p\ i \) by simp
hence \( \text{te}\ p\ i + \beta \leq \text{te}\ p\ (i+1) \) by simp
from this \( \text{corr-p} \) corr-q rts2a have \( \text{te}\ q\ i \leq \text{te}\ p\ (i+1) \)
by blast
thus \( \text{thesis} \) by simp
qed

lemma beta-bound2:
assumes \( \text{corr-p}: \text{correct} \ p \ (\text{te}\ p\ (i+1)) \)
and \( \text{corr-q}: \text{correct} \ q \ (\text{te}\ q\ i) \)
shows \( te p (i+1) - te q i \leq r_{\text{max}} + \beta \)
proof-
from corr-p rte have \( te p i \leq te p (i+1) \)
  by simp
from this corr-p correct-closed have corr-pi: \( \text{correct} p (te p i) \)
  by blast

have split: \( te p (i+1) - te q i = (te p (i+1) - te p i) + (te p i - te q i) \)
  by (simp)

from corr-q corr-pi rts2b have Eq1: \( \text{abs} (te p i - te q i) \leq \beta \)
  by simp
have Eq2: \( te p i - te q i \leq \beta \)
proof cases
  assume \( te q i \leq te p i \)
  from this Eq1 show \( ?\text{thesis} \)
    by (simp add: abs-if)
next
  assume \( \neg (te q i \leq te p i) \)
  from this Eq1 show \( ?\text{thesis} \)
    by (simp add: abs-if)
qed

from corr-p rts0d have \( te p (i+1) - te p i \leq r_{\text{max}} \)
  by simp
from this split Eq2 show \( ?\text{thesis} \) by simp
qed

2.2.2 Bounded-drift for logical clocks (IC)

lemma bd:
  assumes ie: \( s \leq t \)
  and rb1: \( \rho_{\text{bound1}} C \)
  and rb2: \( \rho_{\text{bound2}} D \)
  and PC-ie: \( D q t - D q s \leq C p t - C p s \)
  and corr-p: \( \text{correct} p t \)
  and corr-q: \( \text{correct} q t \)
shows \( |C p t - D q t| \leq |C p s - D q s| + 2*\rho*(t - s) \)
proof-
let \( ?Dt = C p t - D q t \)
let \( ?Ds = C p s - D q s \)
let \( ?Bp = C p t - C p s \)
let \( ?Bq = D q t - D q s \)
let \( ?I = t - s \)

have \( |?Bp - ?Bq| \leq 2*\rho*(t - s) \)
proof-
  from PC-ie have Eq1: \( |?Bp - ?Bq| = ?Bp - ?Bq \) by (simp add: abs-if)
  from corr-p ie rb1 have Eq2: \( ?Bp - ?Bq \leq ?I*(1+\rho) - ?Bq \) (is \( ?E1 \leq ?E2 \))
    by(simp add: rho-bound1-def)
  from corr-q ie rb2 have \( ?I*(1 - \rho) \leq ?Bq \)
    by(simp add: rho-bound2-def)

6
from this have \( \text{Eq3: } \hat{E}_2 \leq \hat{E}_1 + \hat{E}_3 \) by (simp)

have \( \text{Eq4: } \hat{E}_1 = \hat{E}_2 + \hat{E}_3 \) by (simp add: algebra-simps)

from Eq1 Eq2 Eq3 Eq4 show \( \text{thesis by simp} \) qed

moreover have \(|\hat{D}t| \leq |\hat{B}p - \hat{B}q| + |\hat{D}s| \) by (simp add: abs-if)

ultimately show \( \text{thesis by simp} \) qed

lemma bounded-drift:
assumes ie: \( s \leq t \)
and rb1: \( \rho-bound_1 \ C \)
and rb2: \( \rho-bound_2 \ C \)
and rb3: \( \rho-bound_1 \ D \)
and rb4: \( \rho-bound_2 \ D \)
and corr-p: \( \text{correct } p \ t \)
and corr-q: \( \text{correct } q \ t \)
shows \( |C \ p \ t - D \ q \ t| \leq |C \ p \ s - D \ q \ s| + 2\rho(t - s) \)

proof
  let \( \hat{B}p = C \ p \ t - C \ p \ s \)
  let \( \hat{B}q = D \ q \ t - D \ q \ s \)

  show \( \text{thesis} \) proof cases
    assume \( \hat{B}q \leq \hat{B}p \)
    from this ie rb1 rb4 corr-p corr-q bd show \( \text{thesis by simp} \) next
    assume \( \neg(\hat{B}q \leq \hat{B}p) \)
    hence \( \hat{B}p \leq \hat{B}q \) by simp
    from this ie rb2 rb3 corr-p corr-q bd
    have \( |D \ q \ t - C \ p \ t| \leq |D \ q \ s - C \ p \ s| + 2\rho(t - s) \) by simp
    from this show \( \text{thesis by } (\text{simp add: abs-minus-commute}) \) qed

qed

Drift rate of logical clocks

lemma IC-rate1:
rho-bound1 \( (\lambda \ p \ t. \ IC \ p \ i \ t) \)

proof
  { fix \( p::\text{process} \)
    fix \( s::\text{time} \)
    fix \( t::\text{time} \)
    assume cp: \( \text{correct } p \ t \)
    assume ie: \( s \leq t \)
    from cp ie \( \text{correct-closed} \) have cps: \( \text{correct } p \ s \) by blast
    have \( IC \ p \ i \ t - IC \ p \ i \ s \leq (t - s)\rho(t + \rho) \)
    proof
      

7
from \texttt{cp IClock} have \( IC\ p\ i\ t = PC\ p\ t + Adj\ p\ i \)
by \texttt{simp}
moreover
from \texttt{cps IClock} have \( IC\ p\ i\ s = PC\ p\ s + Adj\ p\ i \)
by \texttt{simp}
moreover
from \texttt{cp ie rate-1} have \( PC\ p\ t - PC\ p\ s \leq (t - s)(1 + \rho) \)
by \texttt{simp}
ultimately show \( \texttt{thesis} \) by \texttt{simp}
\texttt{qed}

thus \( \texttt{thesis} \) by (\texttt{simp add: rho-bound1-def})
\texttt{qed}

\textbf{Lemma IC-rate2:}
\textit{rho-bound2} (\( I p\ t.\ IC\ p\ i\ t \))
\textbf{Proof} –
\begin{itemize}
\item fix \( p::\texttt{process} \)
\item fix \( s::\texttt{time} \)
\item fix \( t::\texttt{time} \)
\item assume \( \texttt{cp: correct}\ p\ t \)
\item assume \( ie: s \leq t \)
\item from \( \texttt{cp ie correct-closed} \) have \( \texttt{cps: correct}\ p\ s \)
by \texttt{blast}
\item have \( (t - s)(1 - \rho) \leq IC\ p\ i\ t - IC\ p\ i\ s \)
\textbf{Proof} –
\item from \( \texttt{cp IClock} \) have \( IC\ p\ i\ t = PC\ p\ t + Adj\ p\ i \)
by \texttt{simp}
\item moreover
from \( \texttt{cps IClock} \) have \( IC\ p\ i\ s = PC\ p\ s + Adj\ p\ i \)
by \texttt{simp}
\item moreover
from \( \texttt{cp ie rate-2} \) have \( (t - s)(1 - \rho) \leq PC\ p\ t - PC\ p\ s \)
by \texttt{simp}
ultimately show \( \texttt{thesis} \) by \texttt{simp}
\texttt{qed}
\end{itemize}
thus \( \texttt{thesis} \) by (\texttt{simp add: rho-bound2-def})
\texttt{qed}

Auxiliary function ICf: we introduce this to avoid some unification problem in some tactic of isabelle.

\textbf{Definition}
\textit{ICf}: \( \texttt{nat} \Rightarrow (\texttt{process} \\
\Rightarrow \texttt{time} \\
\Rightarrow \texttt{Clocktime}) \) \textbf{where}
\( ICf\ i = (\lambda\ p\ t.\ IC\ p\ i\ t) \)

\textbf{Lemma IC-bd:}
\textbf{assumes} \( ie: s \leq t \)
\textbf{and} \( corr-p: \texttt{correct}\ p\ t \)
\textbf{and} \( corr-q: \texttt{correct}\ q\ t \)
\textbf{shows} \( |IC\ p\ i\ t - IC\ q\ j\ t| \leq |IC\ p\ i\ s - IC\ q\ j\ s| + 2\rho\ (t - s) \)
\textbf{Proof} –
\textbf{let} \( ?C = ICf\ i \)
let \( ?D = ICf j \)
let \( ?G = | ?C p t - ?D q t | \leq | ?C p s - ?D q s | + 2 * \rho \ast (t - s) \)

from IC-rate1 have rb1: rho-bound1 (ICf i) \land rho-bound1 (ICf j)
  by (simp add: ICf-def)

from IC-rate2 have rb2: rho-bound2 (ICf i) \land rho-bound2 (ICf j)
  by (simp add: ICf-def)

from ie rb1 rb2 corr-p corr-q bounded-drift
have \( ?G \) by simp

from this show \(?thesis\) by (simp add: ICf-def)

qed

lemma event-bound:
assumes ie1: \( 0 \leq (t :: real) \)
and corr-p: correct p t
and corr-q: correct q t
shows \( \exists \ i. \ t < \max (te p i) (te q i) \)
proof (rule ccontr)
  assume A: \( \neg (\exists \ i. \ t < \max (te p i) (te q i)) \)
  show False
  proof
    have F1: \( \forall \ i. \ te p i \leq t \)
    proof
      fix \ i :: nat
      from A have \( \neg (t < \max (te p i) (te q i)) \)
        by simp
      hence Eq1: \( \max (te p i) (te q i) \leq t \) by arith
      have Eq2: \( te p i \leq \max (te p i) (te q i) \)
        by (simp add: max-def)
      from Eq1 Eq2 show \( te p i \leq t \) by simp
    qed
    have F2: \( \forall (i :: nat). \ correct p (te p i) \)
    proof
      fix \ i :: nat
      from F1 have \( te p i \leq t \) by simp
      from this corr-p correct-closed
      show correct p (te p i) by blast
    qed
    have F3: \( \forall (i :: nat). \ real i \ast rmin \leq te p i \)
    proof
      fix \ i :: nat
      show \( real i \ast rmin \leq te p i \)
      proof (induct i)
        from synch0 show \( real (0 :: nat) \ast rmin \leq te p 0 \) by simp
      next
      fix \ i :: nat assume ind-hyp: \( real i \ast rmin \leq te p i \)
      show \( real (Suc i) \ast rmin \leq te p (Suc i) \)
    qed

9
proof –

have Eq1: real i * rmin + rmin = (real i + 1)*rmin
  by (simp add: distrib-right)
have Eq2: real i + 1 = real (i+1) by simp
from Eq1 Eq2
have Eq3: real i * rmin + rmin = real (i+1) * rmin
  by presburger
from F2 have cp1: correct p (te p (i+1))
  by simp
from F2 have cp2: correct p (te p i)
  by simp
from cp1 rts1d have rmin ≤ te p (i+1) - te p i
  by simp
hence Eq4: te p i + rmin ≤ te p (i+1) by simp
from ind-hyp have real i * rmin + rmin ≤ te p i + rmin
  by (simp)
from this Eq4 have real i * rmin + rmin ≤ te p (i+1)
  by simp
from this Eq3 show thesis by simp
qed
qed
qed

have F4: ∀ (i::nat). real i * rmin ≤ t
proof
  fix i::nat
  from F1 have te p i ≤ t by simp
  moreover
  from F3 have real i * rmin ≤ te p i by simp
  ultimately show real i * rmin ≤ t by simp
qed

from constants-ax have 0 < rmin by simp

from this reals-Archimedean3
have Archi: ∃ (k::nat). t < real k * rmin
  by blast

from Archi obtain k::nat where C: t < real k * rmin ..

from F4 have real k * rmin ≤ t by simp
hence notC: ¬ (t < real k * rmin) by simp

from C notC show False by simp
qed
qed

2.3 Agreement property

definition γ1 x = π (2*g*β + 2*Λ) (2*Λ + x + 2*g*(rmax + β))
definition γ2 x = x + 2*g*rmax
definition $\gamma 3 x = \alpha (2 \lambda + x + 2g*(rmax + \beta)) + \lambda + 2g*\beta$

definition

okmaxsync :: [nat, Clocktime] $\Rightarrow$ bool where

okmaxsync i x $\iff$ ($\forall$ p q. correct p (max (te p i) (te q i))
$\wedge$ correct q (max (te p i) (te q i)) $\implies$
$|IC p i (max (te p i) (te q i)) - IC q i (max (te p i) (te q i))| \leq x$)

definition

okClocks :: [process, process, nat] $\Rightarrow$ bool where

okClocks p q i $\iff$ ($\forall$ t. 0 $\leq$ t $\wedge$ t $<$ max (te p i) (te q i))
$\wedge$ correct p t $\wedge$ correct q t
$\implies$ $|VC p t - VC q t| \leq \delta$

lemma okClocks-sym:

assumes ok-pq: okClocks p q i

shows okClocks q p i

proof –

let $?X = PC q i (te p i) - PC q i (te q i)$

from corr-q ic1 PC-monotone have posX: $0 \leq ?X$

by (simp add: le-diff-eq)
from IClock corr-q have \( T1 = \text{cfn} \: q \: (\emptyset \: q \: (i+1)) + \: ?X \)
by(simp add: Adj-def)

from this posX trans-inv show \( ?\)thesis by simp
qed

lemma beta-rho:
assumes ie: \( te \: q \: (i+1) \leq \: te \: p \: (i+1) \)
and corr-p: correct p \( (\: te \: p \: (i+1) \) )
and corr-q: correct q \( (\: te \: p \: (i+1) \) )
and corr-l: correct l \( (\: te \: p \: (i+1) \) )
shows \( |(PC \: l \: (\: te \: p \: (i+1) \)) - PC \: l \: (\: te \: q \: (i+1) \)) - (\: te \: p \: (i+1) - \: te \: q \: (i+1) \)| \( \leq \beta \: \rho \)

proof –
let \( ?X = (PC \: l \: (\: te \: p \: (i+1) \)) - PC \: l \: (\: te \: q \: (i+1) \)) \)
let \( ?D = \: te \: p \: (i+1) - \: te \: q \: (i+1) \)

from ie have posD: \( 0 \leq \: ?D \) by simp

from ie PC-monotone corr-l have posX: \( 0 \leq \: ?X \)
by (simp add: le-diff-eq)

from ie corr-l rate-1 have bound1: \( ?X \leq \: ?D \: (1 + \: \rho) \) by simp
by (blast)

from ie corr-l correct-closed have corr-l-tq: correct l \( (\: te \: q \: (i+1) \) )
by blast

from corr-l-tq corr-p rate-2 have \( |?D| \leq \beta \)
by (simp)

from this constants-ax posD have D-beta: \( ?D \: \rho \leq \beta \: \rho \)
by (simp add: abs-if)

show \( ?\)thesis

proof cases
assume A: \( ?D \leq \: ?X \)
from posX posD A have absEq: \( |?X - \: ?D| = \: ?X - \: ?D \)
by (simp add: abs-if)

from bound1 have bound2: \( ?X - \: ?D \leq \: ?D \: \rho \)
by (simp add: mult.commute distrib-right)

from D-beta absEq bound2 show \( ?\)thesis by simp

next
assume notA: \( \neg (\: ?D \leq \: ?X \) )
from this have absEq2: \( |?X - \: ?D| = \: ?D - \: ?X \)
by (simp add: abs-if)

from ie corr-l rate-2 have bound3: \( ?D \: (1 - \: \rho) \leq \: ?X \) by simp

from this have \( ?D - \: ?X \leq \: ?D \: \rho \) by (simp add: algebra-simps)

from this absEq2 D-beta show \( ?\)thesis by simp

qed

This lemma (and the next one pe-cond2) proves an assumption used in the precision enhancement.

lemma pe-cond1:
assumes ie: \( te \: q \: (i+1) \leq \: te \: p \: (i+1) \)
and corr-p: correct p \( (\: te \: p \: (i+1) \) )
and corr-q: correct q \( (\: te \: p \: (i + 1) \) )
and \( \text{corr-l}: \text{correct} l \ (\text{te} p \ (i+1)) \)

shows \( |\varnothing q \ (i+1) \ l + (PC q \ (\text{te} p \ (i+1)) - PC q \ (\text{te} q \ (i+1))) - \varnothing p \ (i+1) \ l| \leq 2*q*\beta + 2*\Lambda \)

(is \(?M \leq ?N\))

proof –

- let \(?Xl = (PC l \ (\text{te} p \ (i+1)) - PC l \ (\text{te} q \ (i+1)))\)
- let \(?Xq = (PC q \ (\text{te} p \ (i+1)) - PC q \ (\text{te} q \ (i+1)))\)
- let \(?D = \text{te} p \ (i+1) - \text{te} q \ (i+1)\)
- let \(?T = \varnothing p \ (i+1) \ l - \varnothing q \ (i+1) \ l\)
- let \(?RE1 = \varnothing p \ (i+1) \ l - IC l i \ (\text{te} p \ (i+1))\)
- let \(?RE2 = \varnothing q \ (i+1) \ l - IC l i \ (\text{te} q \ (i+1))\)
- let \(?ICT = IC l i \ (\text{te} p \ (i+1)) - IC l i \ (\text{te} q \ (i+1))\)

have \(?M = |(?Xq - ?D) - (?T - ?D)|\)
by(simp add: abs-if)

hence \( \text{Split}: ?M \leq |?Xq - ?D| + |?T - ?D| \)
by(simp add: abs-if)

from \( \text{ie corr-q correct-closed} \) have \( \text{corr-q-tq}: \text{correct} q \ (\text{te} q \ (i+1)) \)
by(blast)

from \( \text{ie corr-l correct-closed} \) have \( \text{corr-l-tq}: \text{correct} l \ (\text{te} q \ (i+1)) \)
by blast

from \( \text{corr-p corr-q corr-l ie beta-rho} \)
have \( XI\text{D}: |?Xl - ?D| \leq \beta*q \)
by simp

from \( \text{corr-p corr-q ie beta-rho} \)
have \( Xq\text{D}: |?Xq - ?D| \leq \beta*q \) by simp

have \( TD: |?T - ?D| \leq 2*\Lambda + \beta*q \)

proof –

- have \( Eq1: |?T - ?D| = |(?T - ?ICT) + (?ICT - ?D)| \) (is \(?E1 = ?E2\))
  by (simp add: abs-if)

- have \( Eq2: |?E2| \leq |?T - ?ICT| + |?ICT - ?D| \)
  by(simp add: abs-if)

- have \( Eq3: |?T - ?ICT| \leq |?RE1| + |?RE2| \)
  by(simp add: abs-if)

from \( \text{readerror corr-p corr-l} \)
have \( Eq4: |?RE1| \leq \Lambda \) by simp

from \( \text{corr-l-tq corr-q-tq this readerror} \)
have \( Eq5: |?RE2| \leq \Lambda \) by simp

from \( Eq3\ Eq4\ Eq5\) have \( Eq6: |?T - ?ICT| \leq 2*\Lambda \)
by simp

have \( Eq7: ?ICT - ?D = ?Xl - ?D \)
proof
from corr-p rte have \( te \, p \, i \leq \, te \, p \, (i+1) \)
by (simp)
from this corr-l correct-closed have corr-l-tpi: \( \text{correct} \, l \, (te \, p \, i) \)
by blast
from corr-q-tq rte have \( te \, q \, i \leq \, te \, q \, (i+1) \)
by simp
from this corr-l-tq correct-closed have corr-l-tqi: \( \text{correct} \, l \, (te \, q \, i) \)
by blast
from IClock corr-l have \( F1: \text{IC} \, l \, i \, (te \, p \, (i+1)) = \text{PC} \, l \, (te \, p \, (i+1)) + \text{Adj} \, l \, i \)
by (simp)
from IClock corr-l-tq have \( F2: \text{IC} \, l \, i \, (te \, q \, (i+1)) = \text{PC} \, l \, (te \, q \, (i+1)) + \text{Adj} \, l \, i \)
by simp
from \( F1 \, F2 \) show \(?thesis\) by (simp)
qed

from this XlD have Eq8: \(|\, ?ICT - \, ?D\, | \leq \beta \ast \varrho \)
by arith
from Eq1 Eq2 Eq6 Eq8 show \(?thesis\)
by (simp)
qed

from Split XqD TD have \( F1: \, ?M \leq 2 \ast \beta \ast \varrho + 2 \ast \Lambda \)
by (simp)
have \( F2: 2 \ast \varrho \ast \beta + 2 \ast \Lambda = 2 \ast \beta \ast \varrho + 2 \ast \Lambda \)
by simp
from \( F1 \) show \(?thesis\) by (simp only: \( F2 \))
qed

lemma pe-cond2:
assumes ic: \( te \, m \, i \leq \, te \, l \, i \)
and corr-k: \( \text{correct} \, k \, (te \, k \, (i+1)) \)
and corr-l-tk: \( \text{correct} \, l \, (te \, k \, (i+1)) \)
and corr-m-tk: \( \text{correct} \, m \, (te \, k \, (i+1)) \)
and ind-hyp: \( |IC \, l \, i \, (te \, l \, i) - IC \, m \, i \, (te \, l \, i)| \leq \delta S \)
shows \(|\, \varnothing \, k \, (i+1) \, l - \, \varnothing \, k \, (i+1) \, m| \leq 2 \ast \Lambda + \delta S + 2 \ast \varrho \ast (rmax + \beta) \)
proof
let \( ?X = \varnothing \, k \, (i+1) \, l - \varnothing \, k \, (i+1) \, m \)
let \( ?N = 2 \ast \Lambda + \delta S + 2 \ast \varrho \ast (rmax + \beta) \)
let \( ?D1 = \varnothing \, k \, (i+1) \, l - IC \, l \, i \, (te \, k \, (i+1)) \)
let \( ?D2 = \varnothing \, k \, (i+1) \, m - IC \, m \, i \, (te \, k \, (i+1)) \)
let \( ?ICS = IC \, l \, i \, (te \, k \, (i+1)) - IC \, m \, i \, (te \, k \, (i+1)) \)
let \( ?tlm = te \, l \, i \)
let \( ?IC = IC \, l \, i \, ?tlm - IC \, m \, i \, ?tlm \)

have Eq1: \(|?X| = |(\, ?D1 - \, ?D2 \, ) + \, ?ICS\, | \, (is \, ?E1 = \, ?E2)\)
by (simp add: abs-if)

have Eq2: \(?E2 \leq |?D1 - \, ?D2| + |?ICS| \, by \, (simp add: abs-if)\)
from corr-l-tk corr-k beta-bound1 have ie-lk: \( t e \ l \ i \leq t e \ k \ (i+1) \) 
by (simp add: le-diff-eq)

from this corr-l-tk correct-closed have corr-l: correct l \( t e \ l \ i \) 
by blast

from ie-lk corr-l-tk corr-m-tk IC-bd have Eq3: \( |ICS| \leq |IC| + 2g*(te k \ (i+1) - tlm) \) 
by simp
from this ind-hyp have Eq4: \( |ICS| \leq \delta S + 2g*(te k \ (i+1) - tlm) \) 
by simp

from corr-l corr-k beta-bound2 have te k \( (i+1) - tlm \leq rmax + \beta \) 
by (simp)
from this constants-ax have 2\( g*(te k \ (i+1) - tlm) \leq 2g*(rmax + \beta) \) 
by (simp add: real-mult-le-cancel-iff2)
from this Eq4 have Eq4a: \( |ICS| \leq \delta S + 2g*(rmax + \beta) \) 
by (simp)

from corr-k corr-l-tk readerror have Eq5: \( |D1| \leq \Lambda \) by simp
from corr-k corr-m-tk readerror have Eq6: \( |D2| \leq \Lambda \) by simp
have \( |D1 - D2| \leq |D1| + |D2| \) by (simp add: abs-if)
from this Eq5 Eq6 have Eq7: \( |D1 - D2| \leq 2\Lambda \) 
by (simp)

from Eq1 Eq2 Eq4a Eq7 split show ?thesis by (simp)
qed

lemma theta-bound:
assumes corr-l: correct l \( t e \ p \ (i+1) \) 
and corr-m: correct m \( t e \ p \ (i+1) \) 
and corr-p: correct p \( t e \ p \ (i+1) \) 
and IC-bound:
  \( |IC \ l \ i \ (max \ (te \ l \ i) \ (te \ m \ i)) - IC \ m \ i \ (max \ (te \ l \ i) \ (te \ m \ i))| \leq \delta S \)
shows \( |\theta \ p \ (i+1) \ l - \theta \ p \ (i+1) \ m| \leq 2\Lambda + \delta S + 2g*(rmax + \beta) \)

proof–
from corr-p corr-l beta-bound1 have tl-le-tp: \( t e \ l \ i \leq t e \ p \ (i+1) \) 
by (simp add: le-diff-eq)
from corr-p corr-m beta-bound1 have tmi-le-tp: \( t e \ m \ i \leq t e \ p \ (i+1) \) 
by (simp add: le-diff-eq)

let \( tml = max \ (te \ l \ i) \ (te \ m \ i) \)
from tl-le-tp tmi-le-tp have tml-le-tp: \( tml \leq t e \ p \ (i+1) \) 
by simp

from tml-le-tp corr-l correct-closed have corr-l-tml: correct l \( tml \) 
by blast
from tml-le-tp corr-m correct-closed have corr-m-tml: correct m \( tml \)
by \texttt{blast}

\texttt{let } \delta Y = 2 \cdot \Lambda + \delta S + 2 \cdot \rho \cdot (r_{\text{max}} + \beta) \\
\texttt{show } |\vartheta p (i+1) l - \vartheta p (i+1) m| \leq \delta Y \\
\texttt{proof cases} \\
\texttt{assume } A: te m i < te l i \\
\texttt{from this IC-bound} \\
\texttt{have } |IC l i (te l i) - IC m i (te l i)| \leq \delta S \\
\texttt{by (simp add: max-def)} \\
\texttt{from this A corr-p corr-l corr-m pe-cond2} \\
\texttt{show } \theta\text{thesis by (simp)} \\
\texttt{next} \\
\texttt{assume } \neg (te m i < te l i) \\
\texttt{hence } Eq1: te l i \leq te m i \text{ by simp} \\
\texttt{from this IC-bound} \\
\texttt{have } Eq2: |IC l i (te m i) - IC m i (te m i)| \leq \delta S \\
\texttt{by (simp add: max-def)} \\
\texttt{hence } |IC m i (te m i) - IC l i (te m i)| \leq \delta S \\
\texttt{by (simp add: abs-minus-commute)} \\
\texttt{from this Eq1 corr-p corr-l corr-m pe-cond2} \\
\texttt{have } |\vartheta p (i+1) m - \vartheta p (i+1) l| \leq \delta Y \\
\texttt{by (simp)} \\
\texttt{thus } \theta\text{thesis by (simp add: abs-minus-commute)} \\
\texttt{qed} \\
\texttt{qed}

\texttt{lemma four-one-ind-half:} \\
\texttt{assumes iec1: } \beta \leq r_{\text{min}} \\
\texttt{and iec2: } \mu \leq \delta S \\
\texttt{and iec3: } \gamma_1 \delta S \leq \delta S \\
\texttt{and ind-hyp: okmaxsync i } \delta S \\
\texttt{and iec4: } te q (i+1) \leq te p (i+1) \\
\texttt{and corr-p: correct p (te p (i+1))} \\
\texttt{and corr-q: correct q (te p (i+1))} \\
\texttt{shows } |IC p (i+1) (te p (i+1)) - IC q (i+1) (te p (i+1))| \leq \delta S \\
\texttt{proof} \\
\texttt{let } ?tpq = te p (i+1) \\
\texttt{let } ?f = \lambda n. \vartheta q (i+1) n + (PC q (te p (i+1)) - PC q (te q (i+1))) \\
\texttt{let } ?g = \vartheta p (i+1) \\
\texttt{from iec4 corr-q correct-closed have corr-q-tq: correct q (te q (i+1))} \\
\texttt{by blast} \\
\texttt{have Eq-IC-cfn: } |IC p (i+1) ?tpq - IC q (i+1) ?tpq| = \\
\texttt{|cfn q ?f - cfn p ?g|} \\
\texttt{proof} \\
\texttt{from corr-p ICp-Suc have Eq1: IC p (i+1) ?tpq = cfn p ?g by simp} \\
\texttt{from iec4 corr-p corr-q IC-trans-inv} \\
\texttt{have Eq2: IC q (i+1) ?tpq = cfn q ?f by simp}
from Eq1 Eq2 show thesis by(simp add: abs-if)
qed

let ?ppred = λ l. correct l (te p (i+1))

let ?X = 2*p*β + 2*Λ
have ∀ l. ?ppred l → |?f l - ?g l| ≤ ?X
proof –
{ fix l
  assume ?ppred l
  from ie4 corr-p corr-q this pe-cond1
  have |?f l - ?g l| ≤ (2*p*β + 2*Λ)
    by (auto)
}
thus thesis by blast
qed

hence cond1: okRead2 ?f ?g ?X ?ppred
  by(simp add: okRead2-def)

let ?Y = 2*Λ + δS + 2*p*(rmax + β)

have ∀ l m. ?ppred l ∧ ?ppred m → |?f l - ?f m| ≤ ?Y
proof –
{ fix l m
  assume corr-l: ?ppred l
  assume corr-m: ?ppred m

  from corr-p corr-l beta-bound1 have tli-le-tp: te l i ≤ te p (i+1)
    by (simp add: le-diff-eq)
  from corr-p corr-m beta-bound1 have tmi-le-tp: te m i ≤ te p (i+1)
    by (simp add: le-diff-eq)

  let ?tlm = max (te l i) (te m i)

  from tli-le-tp tmi-le-tp have tlm-le-tp: ?tlm ≤ te p (i+1)
    by simp

  from ie4 corr-l correct-closed have corr-l-tq: correct l (te q (i+1))
    by blast
  from ie4 corr-m correct-closed have corr-m-tq: correct m (te q (i+1))
    by blast
  from tlm-le-tp corr-l correct-closed have corr-l-tlm: correct l ?tlm
    by blast
  from tlm-le-tp corr-m correct-closed have corr-m-tlm: correct m ?tlm
    by blast

  from ind-hyp corr-l-tlm corr-m-tlm
  have EqAbs1: |IC l i ?tlm - IC m i ?tlm| ≤ δS
    by(auto simp add: okmaxsync-def)
have \( \text{EqAbs3: } |?f l - ?f m| = |\vartheta q (i+1) l - \vartheta q (i+1) m| \)
by (simp add: abs-if)

from \( \text{EqAbs1 corr-q-tq corr-l-tq corr-m-tq theta-bound} \)
have \( |\vartheta q (i+1) l - \vartheta q (i+1) m| \leq ?Y \)
by simp
from this \( \text{EqAbs3} \) have \( |?f l - ?f m| \leq ?Y \)
by simp

thus \( ?\text{thesis by simp} \)
qed

hence \( \text{cond2a: okRead1 ?f ?Y ?ppred by (simp add: okRead1-def)} \)

have \( \forall l m. \ ?ppred l \land \ ?ppred m \longrightarrow |?g l - ?g m| \leq ?Y \)
proof -
{\fix \ l m
\assume \ corr-l: \ ?ppred l
\assume \ corr-m: \ ?ppred m

from \( \text{corr-p corr-l beta-bound1} \) have \( \text{tli-le-tp: } te l i \leq te p (i+1) \)
by (simp add: le-diff-eq)
from \( \text{corr-p corr-m beta-bound1} \) have \( \text{tmi-le-tp: } te m i \leq te p (i+1) \)
by (simp add: le-diff-eq)

let \( ?\text{tlm} = \max (te l i) (te m i) \)
from \( \text{tli-le-tp tmi-le-tp} \) have \( \text{tlm-le-tp: } ?\text{tlm} \leq te p (i+1) \)
by simp

from \( \text{tlm-le-tp corr-l correct-closed} \) have \( \text{corr-l-tlm: } \text{correct l } ?\text{tlm} \)
by blast
from \( \text{tlm-le-tp corr-m correct-closed} \) have \( \text{corr-m-tlm: } \text{correct m } ?\text{tlm} \)
by blast

from \( \text{ind-hyp corr-l-tlm corr-m-tlm} \)
have \( \text{EqAbs1: } |IC l i ?\text{tlm} - IC m i ?\text{tlm}| \leq \delta S \)
by (auto simp add: okmaxsync-def)

from \( \text{EqAbs1 corr-p corr-l corr-m theta-bound} \)
have \( |?g l - ?g m| \leq ?Y \) by simp

thus \( ?\text{thesis by simp} \)
qed

hence \( \text{cond2b: okRead1 ?g ?Y ?ppred by (simp add: okRead1-def)} \)

from \( \text{correct-count} \) have \( \text{np} - \text{maxfaults} \leq \text{count ?ppred np} \)
by simp
from this \( \text{corr-p corr-q cond1 cond2a cond2b prec-enh} \)
have \( |\text{cfn q ?f - cfn p ?g|} \leq \pi ?X ?Y \)
by blast

from \( \text{ie3} \) this have \( |\text{cfn q ?f - cfn p ?g|} \leq \delta S \)
by (simp add: \( \gamma 1\)-def)
from this Eq-IC-cfn show ?thesis by (simp)

qed

Theorem 4.1 in Shankar’s paper.

theorem four-one:
  assumes ie1: \(\beta \leq r_{\min}\)
  and ie2: \(\mu \leq \delta \Sigma\)
  and ie3: \(\gamma_1 \delta \Sigma \leq \delta \Sigma\)
  shows okmaxsync \(i \delta \Sigma\)
proof(induct \(i\))
  show okmaxsync 0 \(\delta \Sigma\)
  proof
  
  \{  
  fix \(p, q\)
  assume corr-p: correct \(p \ (\max (te \ p \ 0) \ (te \ q \ 0))\)
  assume corr-q: correct \(q \ (\max (te \ p \ 0) \ (te \ q \ 0))\)

  from corr-p synch0 have cp0: correct \(p \ 0\) by simp
  from corr-q synch0 have cq0: correct \(q \ 0\) by simp

  from synch0 cp0 cq0 IClock
  have IC-eq-PC:  
  \[|IC \ p \ 0 \ (\max (te \ p \ 0) \ (te \ q \ 0)) − IC \ q \ 0 \ (\max (te \ p \ 0) \ (te \ q \ 0))|\]
  \[= |PC \ p \ 0 − PC \ q \ 0| \ (is \ ?T1 = ?T2)\]
  by(simp add: Adj-def)

  from ie2 init synch0 cp0 have range1: \(0 \leq PC \ p \ 0 \land PC \ p \ 0 \leq \delta \Sigma\)
  by auto
  from ie2 init synch0 cq0 have range2: \(0 \leq PC \ q \ 0 \land PC \ q \ 0 \leq \delta \Sigma\)
  by auto

  have ?T2 \(\leq \delta \Sigma\)
  proof cases
  assume A: PC \(p \ 0 < PC \ q \ 0\)
  from A range1 range2 show ?thesis
  by(auto simp add: abs-if)
  next
  assume notA: \(\neg (PC \ p \ 0 < PC \ q \ 0)\)
  from notA range1 range2 show ?thesis
  by(auto simp add: abs-if)
  qed
  from this IC-eq-PC have ?T1 \(\leq \delta \Sigma\) by simp
  \}
thus ?thesis by (simp add: okmaxsync-def)

qed

next
fix \(i\) assume ind-hyp: okmaxsync \(i \delta \Sigma\)
show okmaxsync \((Suc \ i) \delta \Sigma\)
proof
  
  \{  
  fix \(p, q\)
  assume corr-p: correct \(p \ (\max (te \ p \ (i + 1)) \ (te \ q \ (i + 1)))\)
  assume corr-q: correct \(q \ (\max (te \ p \ (i + 1)) \ (te \ q \ (i + 1)))\)

  from this Eq-IC-cfn show ?thesis by (simp)

qed
let $\: ?tp = \text{te} \: p \: (i + 1) \:
let $\: ?tq = \text{te} \: q \: (i + 1) \:
let $\: ?tpq = \text{max} \: ?tp \: ?tq \:

have $\left| IC \: p \: (i+1) \: ?tpq - IC \: q \: (i+1) \: ?tpq \right| \leq \delta S$ (is $\: ?E1 \leq \delta S$)

proof cases
assume $A: \: ?tq < \: ?tp$
from $A$ corr-p have cp1: correct p $(\text{te} \: p \: (i+1))$
  by (simp add: max-def)
from $A$ corr-q have cq1: correct q $(\text{te} \: p \: (i+1))$
  by (simp add: max-def)
from $A$
have $\text{Eq1: } \: ?E1 = \left| IC \: p \: (i+1) \: (\text{te} \: p \: (i+1)) - IC \: q \: (i+1) \: (\text{te} \: p \: (i+1)) \right|$
  (is $\: ?E1 = \: ?E2$)
  by (simp add: max-def)
from $A$ cp1 cq1 corr-p corr-q ind-hyp ie1 ie2 ie3
  four-one-ind-half
have $\: ?E2 \leq \delta S$ by (simp)
from this $\: \text{Eq1}$ show $\: \text{thesis}$ by simp

next
assume $\neg A: \: \neg (\: ?tq < \: ?tp)$
from this corr-p have cp2: correct p $(\text{te} \: q \: (i+1))$
  by (simp add: max-def)
from $\neg A$ corr-q have cq2: correct q $(\text{te} \: q \: (i+1))$
  by (simp add: max-def)
from $\neg A$
have $\text{Eq2: } \: ?E1 = \left| IC \: q \: (i+1) \: (\text{te} \: q \: (i+1)) - IC \: p \: (i+1) \: (\text{te} \: q \: (i+1)) \right|$
  (is $\: ?E1 = \: ?E3$)
  by (simp add: max-def abs-minus-commute)
from $\neg A$ have $\: ?tp \leq \: ?tq$ by simp
from this $\: \text{cp2} \: \text{cq2} \: \text{ind-hyp} \: ie1 \: ie2 \: ie3 \: \text{four-one-ind-half}$
have $\: ?E3 \leq \delta S$
  by simp
from this $\: \text{Eq2}$ show $\: \text{thesis}$ by (simp)
qed

thus $\: \text{thesis}$ by (simp add: okmaxsync-def)
 qed

qed

lemma VC-cfn:
assumes corr-p: correct p $(\text{te} \: p \: (i+1))$
  and $\: ie: \: \text{te} \: p \: (i+1) < \: \text{te} \: p \: (i+2)$
shows $VC \: p \: (\text{te} \: p \: (i+1)) = cfn \: p \: (\emptyset \: p \: (i+1))$

proof–
from $\: \text{ie} \: corr-p$ VClock have $VC \: p \: (\text{te} \: p \: (i+1)) = IC \: p \: (i+1) \: (\text{te} \: p \: (i+1))$
  by simp
moreover
from corr-p IClock
have $IC \: p \: (i+1) \: (\text{te} \: p \: (i+1)) = PC \: p \: (\text{te} \: p \: (i+1)) + Adj \: p \: (i+1)$
  by blast
moreover
have $PC \: p \: (\text{te} \: p \: (i+1)) + Adj \: p \: (i+1) = cfn \: p \: (\emptyset \: p \: (i+1))$

20
by(simp add: Adj-def)
ultimately show ?thesis by simp
qed

Lemma for the inductive case in Theorem 4.2

lemma four-two-ind:
  assumes ie1: \( \beta \leq rmin \)
  and ie2: \( p \leq S \)
  and ie3: \( \gamma_1 S \leq \delta S \)
  and ie4: \( \gamma_2 S \leq \delta \)
  and ie5: \( \gamma_3 S \leq \delta \)
  and ie6: \( te_q (i+1) \leq te_p (i+1) \)
  and ind-hyp: okClocks p q i
  and t-bound1: \( 0 \leq t \)
  and t-bound2: \( t < max (te_p (i+1)) (te_q (i+1)) \)
  and t-bound3: \( max (te_p i) (te_q i) \leq t \)
  and tpq-bound: \( max (te_p i) (te_q i) < max (te_p (i+1)) (te_q (i+1)) \)
  and corr-p: correct p t
  and corr-q: correct q t
shows \( |VC_p t - VC_q t| \leq \delta \)

proof cases
  assume A: \( t < te_q (i+1) \)
  let \(?tpq\) = \( max (te_p i) (te_q i) \)
  have Eq1: \( te_p i \leq t \land te_q i \leq t \)
  proof cases
    assume te_p i \( \leq \) te_q i
    from this t-bound3 show ?thesis by (simp add: max-def)
  next
    assume \( \neg (te_p i \leq te_q i) \)
    from this t-bound3 show ?thesis by (simp add: max-def)
  qed

from ie6 have tp-max: \( max (te_p (i+1)) (te_q (i+1)) = te_p (i+1) \)
  by(simp add: max-def)
from this t-bound2 have Eq2: \( t < te_p (i+1) \) by simp

from VClock Eq1 Eq2 corr-p have Eq3: \( VC_p t = IC_p i t \) by simp
from VClock Eq1 A corr-q have Eq4: \( VC_q t = IC_q i t \) by simp
from Eq3 Eq4 have Eq5: \( |VC_p t - VC_q t| = |IC_p i t - IC_q i t| \)
  by simp
from t-bound3 corr-p corr-q correct-closed
have corr-tpq: correct p ?tpq \( \land \) correct q ?tpq
  by(blast)
from t-bound3 IC-bl corr-p corr-q
have Eq6: \( |IC_p i t - IC_q i t| \leq |IC_p i ?tpq - IC_q i ?tpq| + 2*\varrho*(t - ?tpq) \) (is \( ?E1 \leq ?E2 \))
  by(blast)
from ie1 ie2 ie3 four-one have okmaxsync i $\delta S$ by simp

from this corr-tpq have $|IC \ p \ ?tpq - IC \ q \ i ?tpq| \leq \delta S$
  by(simp add: okmaxsync-def)

from Eq6 this have Eq7: $?E1 \leq \delta S + 2*\varrho*(t - ?tpq)$ by simp

from corr-p Eq2 rts0 have $t - te \ p \ i \leq \max$ by simp
from this have $t - ?tpq \leq \max$ by (simp add: max-def)
from this constants-ax have $2*\varrho*(t - ?tpq) \leq 2*\varrho*\max$
  by (simp add: real-mult-le-cancel-iff1)
hence $\delta S + 2*\varrho*(t - ?tpq) \leq \delta S + 2*\varrho*\max$
  by simp
from this Eq7 have $?E1 \leq \delta S + 2*\varrho*\max$ by simp
from this Eq5 ie4 show ?thesis by(simp add: $\gamma2$-def)

next
assume $\neg(t < te \ q (i+1))$
hence $B: te \ q (i+1) \leq t$ by simp

from ie6 t-bound2 have tp-max: $\max(te \ p (i+1)) (te \ q (i+1)) = te \ p (i+1)$
  by(simp add: max-def)
have $te \ p \ i \leq \max(te \ p \ i) (te \ q \ i)$
  by(simp add: max-def)

from this t-bound3 have tp-bound1: $te \ p \ i \leq t$ by simp
from tp-max t-bound2 have tp-bound2: $t < te \ p (i+1)$ by simp

have tq-bound1: $t < te \ q (i+2)$
proof (rule ccontr)
  assume $\neg(t < te \ q (i+2))$
hence $C: te \ q (i+2) \leq t$ by simp

from C corr-q correct-closed have corr-q-t2: correct q (te q (i+2)) by blast

have $te \ q (i+1) + \beta \leq t$
proof
  from corr-q-t2 rts1d have $\rmin \leq te \ q (i+2) - te \ q (i+1)$
    by simp
  from this ie1 have $\beta \leq te \ q (i+2) - te \ q (i+1)$
    by simp
  hence $te \ q (i+1) + \beta \leq te \ q (i+2)$ by simp
  from this C show ?thesis by simp
qed
from this corr-p corr-q rts2a have $te \ p (i+1) \leq t$
  by blast
hence $\neg(t < te \ p (i+1))$ by simp
from this tp-bound2 show False by simp
qed
from tq-bound1 B have tq-bound2: \( \text{te} q (i+1) < \text{te} q (i+2) \) by simp
from B tp-bound2 have tq-bound3: \( \text{te} q (i+1) < \text{te} p (i+1) \)
  by simp
from B corr-p correct-closed
have corr-p-tq1: \( \text{correct} p (\text{te} q (i+1)) \) by blast
from B corr-p corr-q correct-closed
have corr-q-tq1: \( \text{correct} q (\text{te} q (i+1)) \) by blast
from B corr-p-tq1 corr-q-tq1 beta-bound1
have tq-bound4: \( \text{te} p i \leq \text{te} q (i+1) \)
  by (simp add: le-diff-eq)
from B VClock B corr-q
have Eq1: \( \text{VC} q t = \text{IC} q (i+1) t \) by simp
from VClock tp-bound1 tp-bound2 corr-p
have Eq2: \( \text{VC} p t = \text{IC} p i t \) by simp
from Eq1 Eq2 have Eq3: \( |\text{VC} p t - \text{VC} q t| = |\text{IC} p i t - \text{IC} q (i+1) t| \)
  by simp
from B corr-p corr-q IC-bd
have |IC p i t - IC q (i+1) t| \( \leq \)
  \( |\text{IC} p i (\text{te} q (i+1)) - \text{IC} q (i+1) (\text{te} q (i+1))| + 2*\rho_s(t - \text{te} q (i+1)) \)
  by simp
from this Eq3
have VC-split: \( |\text{VC} p t - \text{VC} q t| \leq \)
  \( |\text{IC} p i (\text{te} q (i+1)) - \text{IC} q (i+1) (\text{te} q (i+1))| + 2*\rho_s(t - \text{te} q (i+1)) \)
  by simp
from tq-bound2 VClock corr-q-tq1
have Eq4: \( \text{VC} q (\text{te} q (i+1)) = \text{IC} q (i+1) (\text{te} q (i+1)) \) by simp
from this tq-bound2 VClock-cfn corr-q-tq1
have Eq5: \( \text{IC} q (i+1) (\text{te} q (i+1)) = \text{cfn} q (\vartheta q (i+1)) \) by simp
hence \( \text{IC-eq-cfn}: \text{IC} p i (\text{te} q (i+1)) - \text{IC} q (i+1) (\text{te} q (i+1)) = \text{IC} p i (\text{te} q (i+1)) - \text{cfn} q (\vartheta q (i+1)) \)
  (is \( ?E1 = ?E2 \))
  by simp
let \( ?f = \vartheta q (i+1) \)
let \( ?ppred = \lambda l. \text{correct} l (\text{te} q (i+1)) \)
let \( ?X = 2*\Lambda + \delta S + 2*\rho_s(r_{max} + \beta) \)

have \( \forall l m. ?ppred l \land ?ppred m \rightarrow |\vartheta q (i+1) l - \vartheta q (i+1) m| \leq ?X \)
proof
  { fix l :: process
    fix m :: process
    assume corr-l: \( ?ppred l \)
assume corr-m: \( \text{?ppred m} \)

let \( \text{?tlm} = \max \left( \text{te l i} \right) \left( \text{te m i} \right) \)

have tlm-bound: \( \text{?tlm} \leq \text{te q (i+1)} \)

proof –
  from corr-l corr-q-tq1 beta-bound1 have \( \text{te l i} \leq \text{te q (i+1)} \)
    by (simp add: le-diff-eq)
moreover
  from corr-m corr-q-tq1 beta-bound1 have \( \text{te m i} \leq \text{te q (i+1)} \)
    by (simp add: le-diff-eq)
ultimately show \( \text{?thesis by simp} \)
qed

from tlm-bound corr-l corr-m correct-closed
have corr-tlm: correct l \( \text{?tlm} \) ∧ correct m \( \text{?tlm} \)
  by blast

have \(| \text{IC l i ?tlm} - \text{IC m i ?tlm} | \leq \delta S \)

proof –
  from ie1 ie2 ie3 four-one have okmaxsync i \( \delta S \)
    by simp
  from this corr-tlm show \( \text{?thesis by (simp add: okmaxsync-def)} \)
qed

from this corr-l corr-m corr-q-tq1 theta-bound
have \(| \vartheta q (i+1) l - \vartheta q (i+1) m | \leq \alpha \ ?X \ by \ simp \)

thus \( \text{?thesis by blast} \)
qed

hence readOK: okRead1 \( (\vartheta q (i+1)) \ ?X \ ?ppred \)
  by (simp add: okRead1-def)

let \( \text{?E3} = \text{cfn q (\vartheta q (i+1))} - \vartheta q (i+1) p \)
let \( \text{?E4} = \vartheta q (i+1) p - \text{IC p i (te q (i+1))} \)

have \(| \text{?E2} | = | \text{?E3} + \text{?E4} | \)
  by (simp add: abs-if)

hence Eq8: \(| \text{?E2} | \leq | \text{?E3} | + | \text{?E4} | \)
  by (simp add: abs-if)

from correct-count have pppredOK: \( \text{np} - \text{maxfaults} \leq \text{count ?ppred np} \)
  by simp
from readOK pppredOK corr-p-tq1 corr-q-tq1 acc-prsv
have \(| ?E3 | \leq \alpha \ ?X \)
  by blast
from this Eq8 have Eq9: \(| ?E2 | \leq \alpha \ ?X + | ?E4 | \)
  by simp

from corr-p-tq1 corr-q-tq1 readerror
have \(| ?E4 | \leq \Lambda \)

from this Eq9 have Eq10: \(| ?E2 | \leq \alpha \ ?X + \Lambda \)
  by simp

from this VC-split IC-eq-cfn
have almost-right:
\(| \text{VC p t - VC q t} | \leq \)
\[ \alpha \ ?X + \Lambda + 2*\rho*(t - te q (i+1)) \]
by simp

have \( t - te q (i+1) \leq \beta \)
proof (rule ccontr)
assume \( \neg (t - te q (i+1) \leq \beta) \)
then have \( te q (i+1) + \beta \leq t \) by simp
from this corr-p corr-q rts2a have \( te p (i+1) \leq t \)
by auto
then have \( \neg (t < te p (i+1)) \) by simp
from this tp-bound2 show False
by simp
qed

from this constants-ax
have \[ \alpha \ ?X + \Lambda + 2*\rho*(t - te q (i+1)) \]
\[ \leq \alpha \ ?X + \Lambda + 2*\rho*\beta \]
by (simp)

from this almost-right
have \[ |VC p t - VC q t| \leq \alpha \ ?X + \Lambda + 2*\rho*\beta \]
by arith

from this ie5 show ?thesis by (simp add: \( \gamma3\)-def)
qed

Theorem 4.2 in Shankar’s paper.

theorem four-two:
assumes ie1: \( \beta \leq rmin \)
and ie2: \( \mu \leq \delta S \)
and ie3: \( \gamma1 \ \delta S \leq \delta S \)
and ie4: \( \gamma2 \ \delta S \leq \delta \)
and ie5: \( \gamma3 \ \delta S \leq \delta \)
shows okClocks p q i
proof (induct i)
show okClocks p q 0
proof
{ fix \( t :: \text{time} \)
  assume t-bound1: \( 0 \leq t \)
  assume t-bound2: \( t < \text{max} (te p 0) (te q 0) \)
  assume corr-p: correct p t
  assume corr-q: correct q t
  from t-bound2 synch0 have \( t < 0 \)
  by(simp add: max-def)
  from this t-bound1 have False by simp
  hence \[ |VC p t - VC q t| \leq \delta \] by simp
}
thus ?thesis by (simp add: okClocks-def)
qed
next
fix i::nat assume ind-hyp: okClocks p q i
show okClocks p q (Suc i)
proof -
{
  fix t :: time
  assume t-bound1: 0 ≤ t
  assume t-bound2: t < max (te p (i+1)) (te q (i+1))
  assume corr-p: correct p t
  assume corr-q: correct q t
  
  let $?tpq1 = max (te p i) (te q i)
  let $?tpq2 = max (te p (i+1)) (te q (i+1))

  have |VC p t − VC q t| ≤ δ
  proof cases
    assume tpq-bound: $?tpq1 < $?tpq2
    show ?thesis
    proof cases
      assume t < $?tpq1
      from t-bound1 this corr-p corr-q ind-hyp
      show ?thesis by(simp add: okClocks-def)
    next
      assume ¬(t < $?tpq1)
      hence tpq-le-t: $?tpq1 ≤ t by arith
      show ?thesis
      proof cases
        assume A: te q (i+1) ≤ te p (i+1)
        from this tpq-le-t tpq-bound ie1 ie2 ie3 ie4 ie5
        ind-hyp t-bound1 t-bound2
        corr-p corr-q tpq-bound four-two-ind
        show ?thesis by(simp)
      next
        assume B: te p (i+1) ≤ te q (i+1) by simp
        from ind-hyp okClocks-sym have ind-hyp1: okClocks q p i
          by blast
        have maxsym1: max (te p (i+1)) (te q (i+1)) = max (te q (i+1)) (te p (i+1))
          by (simp add: max-def)
        have maxsym2: max (te p i) (te q i) = max (te q i) (te p i)
          by (simp add: max-def)
        from maxsym1 t-bound2
        have t-bound21: t < max (te q (i+1)) (te p (i+1))
          by simp
        from maxsym1 maxsym2 tpq-bound
        have tpq-bound1: max (te q i) (te p i) < max (te q (i+1)) (te p (i+1))
          by simp
        from maxsym2 tpq-le-t
        have tpq-le-t1: max (te q i) (te p i) ≤ t by simp
}

26
\begin{align*}
\text{from } & B \text{ tpq-le-t1 tpq-bound1 ie1 ie2 ie3 ie4 ie5} \\
& \text{ind-hyp1 t-bound1 t-bound21} \\
& \text{corr-p corr-q tpq-bound four-two-ind} \\
\text{have } & |VC q t - VC p t| \leq \delta \text{ by (simp)} \\
\text{thus } & \text{?thesis by (simp add: abs-minus-commute)} \\
\text{qed}
\end{align*}

next
\begin{align*}
\text{assume } & \neg (?tpq1 < ?tpq2) \\
\text{hence } & ?tpq2 \leq ?tpq1 \text{ by arith} \\
\text{from } & t-bound2 \text{ this have } t < ?tpq1 \text{ by arith} \\
\text{from } & t-bound1 \text{ this corr-p corr-q ind-hyp} \\
\text{show } & \text{?thesis by (simp add: okClocks-def)} \\
\text{qed}
\end{align*}

\begin{align*}
\text{thus } & \text{?thesis by (simp add: okClocks-def)} \\
\text{qed}
\end{align*}

The main theorem: all correct clocks are synchronized within the bound \( \delta \).

\begin{align*}
\text{theorem } & \text{agreement:} \\
\text{assumes } & \text{ie1: } \beta \leq \text{rmin} \\
\text{and } & \text{ie2: } \mu \leq \delta S \\
\text{and } & \text{ie3: } \gamma_1 \delta S \leq \delta S \\
\text{and } & \text{ie4: } \gamma_2 \delta S \leq \delta \\
\text{and } & \text{ie5: } \gamma_3 \delta S \leq \delta \\
\text{and } & \text{ie6: } 0 \leq t \\
\text{and } & \text{cpq: correct p t \& correct q t} \\
\text{shows } & |VC p t - VC q t| \leq \delta \\
\text{proof} & - \\
\text{from } & \text{ie6 cpq event-bound have } \exists i :: \text{nat. } t < \max (te p i) (te q i) \\
& \text{by simp} \\
\text{from } & \text{this obtain } i :: \text{nat where t-bound: } t < \max (te p i) (te q i) ..
\end{align*}

\begin{align*}
\text{from } & t-bound \text{ ie1 ie2 ie3 ie4 ie5 four-two have okClocks p q i} \\
& \text{by simp} \\
\text{from } & \text{ie6 this t-bound cpq show } \text{?thesis} \\
& \text{by (simp add: okClocks-def)} \\
\text{qed}
\end{align*}

end

References

