Some Properties of FBA Systems

Giuliano Losa

September 3, 2019

Contents

theory *FBA*
imports *Main*
begin

1 Personal Byzantine quorum systems

We start by proving some facts about an abstraction of FBA called a personal Byzantine quorum system (PBQS). For more details about PBQSs see the paper "Stellar Consensus by Instantiation", to appear at DISC 2019.

locale *personal-quorums* =
fixes *quorum-of* :: *'node* ⇒ *'node set* ⇒ *bool*
assumes *quorum-assm*: $\bigwedge p\ p'\ .\ [\![p \in W;\ \mathit{quorum\text{-}of}\ p\ Q;\ p' \in Q \cap W]\!] \Longrightarrow \exists\ Q'\ .\ \mathit{quorum\text{-}of}\ p'\ Q' \wedge Q' \subseteq Q$
— In other words, a quorum (of some participant) must contain a quorum of each of its members.
begin

definition *blocks* **where**
— Set R blocks participant p.
$\mathit{blocks}\ R\ p \equiv \forall\ Q\ .\ \mathit{quorum\text{-}of}\ p\ Q \longrightarrow Q \cap R \neq \{\}$

abbreviation *blocked-by* **where** $\mathit{blocked\text{-}by}\ R \equiv \{p\ .\ \mathit{blocks}\ R\ p\}$

lemma *blocked-blocked-subset-blocked*:
$\mathit{blocked\text{-}by}\ (\mathit{blocked\text{-}by}\ R) \subseteq \mathit{blocked\text{-}by}\ R$
proof −
have *False* **if** $p \in \mathit{blocked\text{-}by}\ (\mathit{blocked\text{-}by}\ R)$ **and** $p \notin \mathit{blocked\text{-}by}\ R$ **for** p

proof $-$
have $1{:}Q \cap \mathit{blocked\text{-}by}\ R \neq \{\}$ **if** $\mathit{quorum\text{-}of}\ p\ Q$ **for** Q
using $\langle p \in \mathit{blocked\text{-}by}\ (\mathit{blocked\text{-}by}\ R)\rangle$ *that* **unfolding** *blocks-def* **by** *auto*
have $Q \cap R \neq \{\}$ **if** $\mathit{quorum\text{-}of}\ p\ Q$ **for** Q
proof $-$
obtain p' **where** $p' \in \mathit{blocked\text{-}by}\ R$ **and** $p' \in Q$
using 1 $\langle \mathit{quorum\text{-}of}\ p\ Q\rangle$ **by** *auto*
then obtain Q' **where** $\mathit{quorum\text{-}of}\ p'\ Q'$ **and** $Q' \subseteq Q$
using *quorum-assm that* $\langle \mathit{quorum\text{-}of}\ p\ Q\rangle$ **by** *blast*
with $\langle p' \in \mathit{blocked\text{-}by}\ R\rangle$ **show** $Q \cap R \neq \{\}$
using *blocks-def* **by** *fastforce*
qed
hence $p \in \mathit{blocked\text{-}by}\ R$ **by** $(\mathit{simp\ add}{:}\ \mathit{blocks\text{-}def})$
thus *False* **using** $\mathit{that}(2)$ **by** *auto*
qed
thus $\mathit{blocked\text{-}by}\ (\mathit{blocked\text{-}by}\ R) \subseteq \mathit{blocked\text{-}by}\ R$
by *blast*
qed

end

We now add the set of correct nodes to the model.

locale $\mathit{with\text{-}w} = \mathit{personal\text{-}quorums}\ \mathit{quorum\text{-}of}$ **for** $\mathit{quorum\text{-}of} :: {}'\mathit{node} \Rightarrow {}'\mathit{node\ set} \Rightarrow \mathit{bool}\ +$
fixes $W{::}'\mathit{node\ set}$
begin

abbreviation B **where** $B \equiv -W$
— B is the set of malicious nodes.

definition *quorum-of-set* **where** $\mathit{quorum\text{-}of\text{-}set}\ S\ Q \equiv \exists\ p \in S\ .\ \mathit{quorum\text{-}of}\ p\ Q$

1.1 The set of participants not blocked by malicious participants

definition L **where** $L \equiv W - (\mathit{blocked\text{-}by}\ B)$

lemma $\mathit{l2}$: $p \in L \Longrightarrow \exists\ Q \subseteq W.\ \mathit{quorum\text{-}of}\ p\ Q$
unfolding *L-def blocks-def* **using** *DiffD2* **by** *auto*

lemma $\mathit{l3}$:
— If a participant is not blocked by the malicious participants, then it has a quorum consisting exclusively of correct participants which are not blocked by the malicious participants.
assumes $p \in L$ **shows** $\exists\ Q \subseteq L\ .\ \mathit{quorum\text{-}of}\ p\ Q$
proof $-$
have *False* **if** $1{:}\bigwedge\ Q\ .\ \mathit{quorum\text{-}of}\ p\ Q \Longrightarrow Q \cap (-L) \neq \{\}$
proof $-$
obtain Q **where** $\mathit{quorum\text{-}of}\ p\ Q$ **and** $Q \subseteq W$

using $\mathit{l2}$ $\langle p \in L \rangle$ **by** *auto*
obtain p' **where** $p' \in Q \cap (-L)$ **using** *1* $\langle$*quorum-of* p $Q\rangle$ **by** *auto*
then obtain Q' **where** *quorum-of* p' Q' **and** $Q' \subseteq Q$ **using** $\langle$*quorum-of* p $Q\rangle$ *quorum-assm* **by** *blast*

from $\langle$*quorum-of* p' $Q'\rangle$ **and** $\langle p' \in Q \cap (-L)\rangle$ $\langle Q \subseteq W\rangle$ **have** $Q' \cap B \neq \{\}$ **unfolding** *L-def blocks-def* **by** *auto*
thus *False* **using** $\langle Q \subseteq W\rangle$ $\langle Q' \subseteq Q\rangle$ **by** *auto*
qed
thus *?thesis* **by** (*metis disjoint-eq-subset-Compl double-complement*)
qed

1.2 Consensus clusters and intact sets

definition *is-intertwined* **where**
is-intertwined $S \equiv S \subseteq W$
$\wedge$ ($\forall$ Q Q' . *quorum-of-set* S Q $\wedge$ *quorum-of-set* S $Q' \longrightarrow W \cap Q \cap Q' \neq \{\}$)

definition *is-intact* **where**
— This is equivalent to the notion of intact set presented in the Stellar Whitepaper [**?**]
is-intact $I \equiv I \subseteq W \wedge (\forall\ p \in I\ .\ \exists\ Q \subseteq I\ .$ *quorum-of* p Q)
$\wedge$ ($\forall$ Q Q' . *quorum-of-set* I Q $\wedge$ *quorum-of-set* I $Q' \longrightarrow I \cap Q \cap Q' \neq \{\}$)

Next we show that the union of two intact sets that intersect is an intact set.

lemma *intact-union*:
assumes *is-intact* I_1 **and** *is-intact* I_2 **and** $I_1 \cap I_2 \neq \{\}$
shows *is-intact* $(I_1 \cup I_2)$
proof $-$
have $I_1 \cup I_2 \subseteq W$
using *assms*(*1*) *assms*(*2*) *is-intact-def* **by** *auto*
moreover
have $\forall\ p \in (I_1 \cup I_2)\ .\ \exists\ Q \subseteq (I_1 \cup I_2)$. *quorum-of* p Q
using $\langle$*is-intact* $I_1\rangle$ $\langle$*is-intact* $I_2\rangle$ **unfolding** *is-intact-def*
by (*meson UnE le-supI1 le-supI2*)
moreover
have $(I_1 \cup I_2) \cap Q_1 \cap Q_2 \neq \{\}$
if *quorum-of-set* $(I_1 \cup I_2)$ Q_1 **and** *quorum-of-set* $(I_1 \cup I_2)$ Q_2
for Q_1 Q_2
proof $-$
have $(I_1 \cup I_2) \cap Q_1 \cap Q_2 \neq \{\}$ **if** *quorum-of-set* I Q_1 **and** *quorum-of-set* I Q_2 **and** $I = I_1 \vee I = I_2$ **for** I
using $\langle$*is-intact* $I_1\rangle$ $\langle$*is-intact* $I_2\rangle$ $\langle$*quorum-of-set* $(I_1 \cup I_2)$ $Q_1\rangle$ $\langle$*quorum-of-set* $(I_1 \cup I_2)$ $Q_2\rangle$ *that*
unfolding *quorum-of-set-def is-intact-def*
by (*metis inf-assoc inf-bot-right inf-sup-absorb sup-commute*)
moreover
have $\langle (I_1 \cup I_2) \cap Q_1 \cap Q_2 \neq \{\}\rangle$ **if** *is-intact* I_1 **and** *is-intact* I_2

and $I_1 \cap I_2 \neq \{\}$ **and** *quorum-of-set* I_1 Q_1 **and** *quorum-of-set* I_2 Q_2
for I_1 I_2 — We generalize to avoid repeating the argument twice
proof –
obtain p Q **where** *quorum-of* p Q **and** $p \in I_1 \cap I_2$ **and** $Q \subseteq I_2$
using ‹$I_1 \cap I_2 \neq \{\}$› ‹*is-intact* I_2› **unfolding** *is-intact-def* **by** *blast*
have $Q \cap Q_1 \neq \{\}$ **using** ‹*is-intact* I_1› ‹*quorum-of-set* I_1 Q_1› ‹*quorum-of* p Q› ‹$p \in I_1 \cap I_2$›
unfolding *is-intact-def quorum-of-set-def*
by (*metis Int-assoc Int-iff inf-bot-right*)
then obtain $Q_1{}'$ **where** *quorum-of-set* I_2 $Q_1{}'$ **and** $Q_1{}' \subseteq Q_1$
using ‹$Q \subseteq I_2$› ‹*quorum-of-set* I_1 Q_1› *quorum-assm* **unfolding** *quorum-of-set-def* **by** *blast*
thus $(I_1 \cup I_2) \cap Q_1 \cap Q_2 \neq \{\}$ **using** ‹*is-intact* I_2› ‹*quorum-of-set* I_2 Q_2›
unfolding *is-intact-def* **by** *blast*
qed
ultimately show *?thesis* **using** *assms that* **unfolding** *quorum-of-set-def* **by** *auto*
qed
ultimately show *?thesis* **using** *assms*
unfolding *is-intact-def* **by** *simp*
qed

end

2 Stellar quorum systems

We now show that FBA gives rise to a PBQS, and thus that the properties of PBQSs hold in FBA, and we prove the cascade theorem.

locale *stellar* =
fixes *slices* :: *'node* ⇒ *'node set set* — the quorum slices
and W :: *'node set* — the well-behaved nodes
assumes *slices-ne*: $\bigwedge p\ .\ p \in W \Longrightarrow$ *slices* $p \neq \{\}$
begin

definition *quorum* **where**
quorum $Q \equiv \forall\ p \in Q \cap W\ .\ (\exists\ Sl \in$ *slices* $p\ .\ Sl \subseteq Q)$

definition *quorum-of* **where** *quorum-of* p $Q \equiv$ *quorum* $Q \wedge (p \notin W \vee (\exists\ Sl \in$ *slices* $p\ .\ Sl \subseteq Q))$

lemma *quorum-union*:*quorum* $Q \Longrightarrow$ *quorum* $Q' \Longrightarrow$ *quorum* $(Q \cup Q')$
unfolding *quorum-def*
by (*metis IntE Int-iff UnE inf-sup-aci(1) sup.coboundedI1 sup.coboundedI2*)

lemma *l1*:
assumes $\bigwedge\ p\ .\ p \in S \Longrightarrow \exists\ Q \subseteq S\ .$ *quorum-of* p Q **and** $p \in S$
shows *quorum-of* p S **using** *assms* **unfolding** *quorum-of-def quorum-def*
by (*meson Int-iff subset-trans*)

lemma *is-pbqs*:
assumes *quorum-of* p Q **and** $p' \in Q$
shows *quorum-of* p' Q
— This is the property required of a PBQS.
using *assms*
by (*simp add*: *quorum-def quorum-of-def*)

interpretation *with-w quorum-of*
— Stellar quorums form a personal quorum system.
unfolding *with-w-def personal-quorums-def*
quorum-def quorum-of-def **by** *blast*

lemma *quorum-is-quorum-of-some-slice*:
assumes *quorum-of* p Q **and** $p \in W$
obtains S **where** $S \in$ *slices* p **and** $S \subseteq Q$
and $\bigwedge p' .\ p' \in S \cap W \Longrightarrow$ *quorum-of* p' Q
using *assms* **unfolding** *quorum-def quorum-of-def* **by** *fastforce*

lemma *is-intact* $C \Longrightarrow$ *quorum* C
— Every intact set is a quorum.
unfolding *is-intact-def quorum-of-def quorum-def*
by *fastforce*

lemma *in-quorum*:*quorum* $Q \Longrightarrow p \in Q \Longrightarrow$ *quorum-of* p Q
by (*simp add*: *quorum-def quorum-of-def*)

2.1 Properties of blocking sets

inductive *blocking-max* **where**
— This is the set of participants that are eventually blocked by a set R when byzantine processors help epidemic propagation.
$[\![p \in W;\ \forall\ Sl \in \textit{slices}\ p\ .\ \exists\ q \in Sl\ .\ q \in R \cup B \lor \textit{blocking-max}\ R\ q]\!] \Longrightarrow \textit{blocking-max}\ R\ p$
inductive-cases *blocking-max* R p

Next we show that if R blocks p and p belongs to an intact set cluster S, then $R \cap S \neq \{\}$.

We first prove two auxiliary lemmas:

lemma *intact-wb*:$p \in I \Longrightarrow$ *is-intact* $I \Longrightarrow p \in W$
using *is-intact-def* **by** *fastforce*

lemma *intact-has-ne-slices*:
assumes *is-intact* I **and** $p \in I$
and $Sl \in$ *slices* p
shows $Sl \neq \{\}$
using *assms* **unfolding** *is-intact-def quorum-of-set-def quorum-of-def quorum-def*
by (*metis empty-iff inf-bot-left inf-bot-right subset-refl*)

lemma *intact-has-intact-slice*:
assumes *is-intact* I **and** $p \in I$
obtains Sl **where** $Sl \in$ *slices* p **and** $Sl \subseteq I$
using *assms* **unfolding** *is-intact-def quorum-of-set-def quorum-of-def quorum-def*
by (*metis Int-commute empty-iff inf.order-iff inf-bot-right le-infI1*)

theorem *blocking-max-intersects-intact*:
— if R blocks p when malicious participants help epidemic propagation, and p belongs to an intact set S, then $R \cap S \neq \{\}$
assumes *blocking-max* R p **and** *is-intact* S **and** $p \in S$
shows $R \cap S \neq \{\}$ **using** *assms*
proof (*induct*)
case (*1* p R)
obtain Sl **where** $Sl \in$ *slices* p **and** $Sl \subseteq S$ **using** *intact-has-intact-slice*
using *1.prems* **by** *blast*
moreover have $Sl \subseteq W$ **using** *assms*(*2*) *calculation*(*2*) *is-intact-def* **by** *auto*
ultimately show *?case*
using *1.hyps assms*(*2*) **by** *fastforce*
qed

We now prove the cascade theorem

theorem *cascade-thm*:
assumes *is-intact* I **and** $p \in I$ **and** *quorum-of* p Q **and** $Q \subseteq S$
obtains $I \subseteq S \mid \exists\ p' \in (W - S)\ .\ (\forall\ s \in$ *slices* $p'\ .\ s \cap S \cap W \neq \{\})$
proof −
have *False* **if** *1*:$\forall\ p' \in (W - S)\ .\ (\exists\ s \in$ *slices* $p'\ .\ s \cap S \cap W = \{\})$ **and** *2*:$\neg I \subseteq S$
proof −
have $I \subseteq W$ **using** *assms*(*1*) *is-intact-def* **by** *auto*
with *1* **have** *quorum* $((-S) \cup B)$ **unfolding** *quorum-def* **using** *Int-commute* **by** *fastforce*
with *2* **obtain** q **where** $q \in I$ **and** *quorum-of* q $((-S) \cup B)$ **using** *in-quorum* **by** *fastforce*
moreover have $((-S) \cup B) \cap Q \subseteq B$ **using** *Compl-anti-mono* ‹$Q \subseteq S$› **by** *blast*
ultimately show *False* **using** ‹$p \in I$› **and** ‹*quorum-of* p Q› **and** ‹*is-intact* I›
unfolding *is-intact-def quorum-of-set-def* **by** *blast*
qed
thus *?thesis* **using** *that* **by** *blast*
qed

end

end