Stellar Quorum Systems

Giuliano Losa
Galois, Inc., USA
giuliano@galois.com

March 19, 2025

Abstract

We formalize the static properties of personal Byzantine quorum systems (PBQSs) and Stellar quorum systems, as described in the paper "Stellar Consensus by Reduction", to appear at DISC 2019.

Contents

This theory formalizes some of the results appearing in the paper "Stellar Consensus By Reduction"[1]. We prove static properties of personal Byzantine quorum systems and Stellar quorum systems.

theory *Stellar-Quorums*
  imports *Main*
begin

1 Personal Byzantine quorum systems

locale *personal-quorums* =
  fixes $quorum\text{-}of :: 'node \Rightarrow 'node\ set \Rightarrow bool$
  assumes $quorum\text{-}assm{:}\bigwedge\ p\ p'\ .\ [\![quorum\text{-}of\ p\ Q;\ p' \in Q]\!] \Longrightarrow quorum\text{-}of\ p'\ Q$
  — In other words, a quorum (of some participant) is a quorum of all its members.
begin

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

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

lemma *blocked-blocked-subset-blocked*:
  $blocked\text{-}by\ (blocked\text{-}by\ R) \subseteq blocked\text{-}by\ R$
⟨*proof*⟩

end

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

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

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

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

1.1 The set of participants not blocked by malicious participants

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

lemma *l2*: $p \in L \Longrightarrow \exists\ \ Q\ \ \subseteq\ W.\ quorum\text{-}of\ p\ Q$
  ⟨*proof*⟩

lemma *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** $\exists\ Q \subseteq L$. *quorum-of* p Q
⟨*proof*⟩

1.2 Consensus clusters and intact sets

definition *is-intertwined* **where**
— This definition is not used in this theory, but we include it to formalize the notion of intertwined set appearing in the DISC paper.
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-cons-cluster* **where**
— Consensus clusters
is-cons-cluster $C \equiv C \subseteq W \wedge (\forall\ p \in C\ .\ \exists\ Q \subseteq C$. *quorum-of* p $Q)$
$\wedge$ $(\forall\ Q\ Q'$. *quorum-of-set* C Q $\wedge$ *quorum-of-set* C $Q' \longrightarrow W \cap Q \cap Q' \neq \{\})$

definition *strong-consensus-cluster* **where**
strong-consensus-cluster $I \equiv I \subseteq W \wedge (\forall\ p \in I\ .\ \exists\ Q \subseteq I$. *quorum-of* p $Q)$
$\wedge$ $(\forall\ Q\ Q'$. *quorum-of-set* I Q $\wedge$ *quorum-of-set* I $Q' \longrightarrow I \cap Q \cap Q' \neq \{\})$

lemma *strong-consensus-cluster-imp-cons-cluster*:
— Every intact set is a consensus cluster
shows *strong-consensus-cluster* $I \Longrightarrow$ *is-cons-cluster* I
⟨*proof*⟩

lemma *cons-cluster-neq-cons-cluster*:
— Some consensus clusters are not strong consensus clusters and have no superset that is a strong consensus cluster.
shows *is-cons-cluster* $I \wedge (\forall\ J\ .\ I \subseteq J \longrightarrow \neg$*strong-consensus-cluster* $J)$ **nitpick**[*falsify=false*, *card 'node=3*, *expect=genuine*]
⟨*proof*⟩

Next we show that the union of two consensus clusters that intersect is a consensus cluster.

theorem *cluster-union*:
assumes *is-cons-cluster* C_1 **and** *is-cons-cluster* C_2 **and** $C_1 \cap C_2 \neq \{\}$
shows *is-cons-cluster* $(C_1 \cup C_2)$
⟨*proof*⟩

Similarly, the union of two strong consensus clusters is a strong consensus cluster.

lemma *strong-cluster-union*:
assumes *strong-consensus-cluster* C_1 **and** *strong-consensus-cluster* C_2 **and** $C_1 \cap C_2 \neq \{\}$
shows *strong-consensus-cluster* $(C_1 \cup C_2)$
⟨*proof*⟩

end

2 Stellar quorum systems

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* $p\ .\ Sl \subseteq Q))$
— TODO: $p \notin W$ needed?

lemma *quorum-union*:*quorum* $Q \Longrightarrow$ *quorum* $Q' \Longrightarrow$ *quorum* $(Q \cup Q')$
⟨*proof*⟩

lemma *l1*:
assumes $\bigwedge\ p\ .\ p \in S \Longrightarrow \exists\ Q \subseteq S\ .$ *quorum-of* $p\ Q$ **and** $p \in S$
shows *quorum-of* $p\ S$ ⟨*proof*⟩

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.
⟨*proof*⟩

interpretation *with-w quorum-of*
— Stellar quorums form a personal quorum system.
⟨*proof*⟩

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* $p'\ Q$
⟨*proof*⟩

lemma *is-cons-cluster* $C \Longrightarrow$ *quorum* C
— Every consensus cluster is a quorum.
⟨*proof*⟩

2.1 Properties of blocking sets

inductive *blocking-min* **where**
— This is the set of correct participants that are eventually blocked by a set R when byzantine processors do not take steps.

$\llbracket p \in W;\ \forall\ Sl \in slices\ p\ .\ \exists\ q \in Sl \cap W\ .\ q \in R \lor blocking\text{-}min\ R\ q \rrbracket \Longrightarrow blocking\text{-}min\ R\ p$

inductive-cases *blocking-min-elim*:*blocking-min R p*

inductive *blocking-max* **where**

— This is the set of participants that are eventually blocked by a set *R* when byzantine processors help epidemic propagation.

$\llbracket p \in W;\ \forall\ Sl \in slices\ p\ .\ \exists\ q \in Sl\ .\ q \in R \cup B \lor blocking\text{-}max\ R\ q \rrbracket \Longrightarrow blocking\text{-}max\ R\ p$

inductive-cases *blocking-max R p*

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

We first prove two auxiliary lemmas:

lemma *cons-cluster-wb*:$p \in C \Longrightarrow$ *is-cons-cluster* $C \Longrightarrow p \in W$
⟨*proof*⟩

lemma *cons-cluster-has-ne-slices*:
assumes *is-cons-cluster C* **and** $p \in C$
and $Sl \in slices\ p$
shows $Sl \neq \{\}$
⟨*proof*⟩

lemma *cons-cluster-has-cons-cluster-slice*:
assumes *is-cons-cluster C* **and** $p \in C$
obtains *Sl* **where** $Sl \in slices\ p$ **and** $Sl \subseteq C$
⟨*proof*⟩

theorem *blocking-max-intersects-intact*:
— if *R* blocks *p* when malicious participants help epidemic propagation, and *p* belongs to a consensus cluster *C*, then $R \cap C \neq \{\}$
assumes *blocking-max R p* **and** *is-cons-cluster C* **and** $p \in C$
shows $R \cap C \neq \{\}$ ⟨*proof*⟩

Now we show that if $p \in C$, C is a consensus cluster, and quorum Q is such that $Q \cap C \neq \{\}$, then $Q \cap W$ blocks p.

We start by defining the set of participants reachable from a participant through correct participants. Their union trivially forms a quorum. Moreover, if p is not blocked by a set R, then we show that the set of participants reachable from p and not blocked by R forms a quorum disjoint from R. It follows that if p is a member of a consensus cluster C and Q is a quorum of a member of C, then $Q \cap W$ must block p, as otherwise quorum intersection would be violated.

inductive *not-blocked* **for** *p R* **where**

$\llbracket Sl \in slices\ p;\ \forall\ q \in Sl \cap W\ .\ q \notin R \land \neg blocking\text{-}min\ R\ q;\ q \in Sl \rrbracket \Longrightarrow not\text{-}blocked\ p\ R\ q$

| ⟦*not-blocked* p R p'; $p' \in W$; *Sl* $\in$ *slices* p'; $\forall$ $q \in Sl \cap W$. $q \notin R \wedge \neg$*blocking-min* R q; $q \in Sl$⟧ $\Longrightarrow$ *not-blocked* p R q
inductive-cases *not-blocked-cases*:*not-blocked* p R q

lemma *l4*:
  fixes Q p R
  defines $Q \equiv \{q$. *not-blocked* p R $q\}$
  shows *quorum* Q
⟨*proof*⟩

lemma *l5*:
  fixes Q p R
  defines $Q \equiv \{q$. *not-blocked* p R $q\}$
  assumes $\neg$*blocking-min* R p **and** ‹$p \in C$› **and** ‹*is-cons-cluster* C›
  shows *quorum-of* p Q
⟨*proof*⟩

lemma *cons-cluster-ne-slices*:
  assumes *is-cons-cluster* C **and** $p \in C$ **and** *Sl* $\in$ *slices* p
  shows *Sl*$\neq\{\}$
  ⟨*proof*⟩

lemma *l6*:
  fixes Q p R
  defines $Q \equiv \{q$. *not-blocked* p R $q\}$
  shows $Q \cap R \cap W = \{\}$
⟨*proof*⟩

theorem *quorum-blocks-cons-cluster*:
  assumes *quorum-of-set* C Q **and** $p \in C$ **and** *is-cons-cluster* C
  shows *blocking-min* $(Q \cap W)$ p
⟨*proof*⟩

2.2 Reachability through a set

Here we define the part of a quorum Q of p that is reachable through correct participants from p. We show that if p and p' are members of the same consensus cluster and Q is a quorum of p and Q' is a quorum of p', then the intersection $Q \cap Q' \cap W$ is reachable from both p and p' through the consensus cluster.

inductive *reachable-through* **for** p S **where**
  reachable-through p S p
| ⟦*reachable-through* p S p'; $p' \in W$; *Sl* $\in$ *slices* p'; *Sl* $\subseteq S$; $p'' \in Sl$⟧ $\Longrightarrow$ *reachable-through* p S p''

definition *truncation* **where** *truncation* p S $\equiv \{p'$. *reachable-through* p S $p'\}$

lemma *l13*:
assumes *quorum-of* p Q **and** $p \in W$ **and** *reachable-through* p Q p'
shows *quorum-of* p' Q
⟨*proof*⟩

lemma *l14*:
assumes *quorum-of* p Q **and** $p \in W$
shows *quorum* (*truncation* p Q)
⟨*proof*⟩

lemma *l15*:
assumes *is-cons-cluster* I **and** *quorum-of* p Q **and** *quorum-of* p' Q' **and** $p \in I$ **and** $p' \in I$ **and** $Q \cap Q' \cap W \neq \{\}$
shows $W \cap$ (*truncation* p Q) $\cap$ (*truncation* p' Q') $\neq \{\}$
⟨*proof*⟩

end

2.3 Elementary quorums

In this section we define the notion of elementary quorum, which is a quorum that has no strict subset that is a quorum. It follows directly from the definition that every finite quorum contains an elementary quorum. Moreover, we show that if Q is an elementary quorum and n_1 and n_2 are members of Q, then n_2 is reachable from n_1 in the directed graph over participants defined as the set of edges (n, m) such that m is a member of a slice of n. This lemma is used in the companion paper to show that probabilistic leader-election is feasible.

locale *elementary* = *stellar*
begin

definition *elementary* **where**
elementary $s \equiv$ *quorum* $s \wedge (\forall\ s'\ .\ s' \subset s \longrightarrow \neg$*quorum* $s')$

lemma *finite-subset-wf*:
shows *wf* $\{(X, Y).\ X \subset Y \wedge$ *finite* $Y\}$
⟨*proof*⟩

lemma *quorum-contains-elementary*:
assumes *finite* s **and** $\neg$ *elementary* s **and** *quorum* s
shows $\exists\ s'\ .\ s' \subset s \wedge$ *elementary* s' ⟨*proof*⟩

inductive *path* **where**
path []
| $\bigwedge x$. *path* $[x]$
| $\bigwedge l\ n$. ⟦*path* l; $S \in Q$ (*hd* l); $n \in S$⟧ $\Longrightarrow$ *path* $(n\#l)$

theorem *elementary-connected*:

assumes *elementary s* **and** $n_1 \in s$ **and** $n_2 \in s$ **and** $n_1 \in W$ **and** $n_2 \in W$
shows $\exists\ l\ .\ hd\ (rev\ l) = n_1 \wedge hd\ l = n_2 \wedge path\ l$ (**is** *?P*)
⟨*proof*⟩

end

2.4 The intact sets of the Stellar Whitepaper

definition *project* **where**
project slices S n $\equiv \{Sl \cap S \mid Sl\ .\ Sl \in slices\ n\}$
— Projecting on S is the same as deleting the complement of S, where deleting is understood as in the Stellar Whitepaper.

2.4.1 Intact and the Cascade Theorem

locale *intact* = — Here we fix an intact set I and prove the cascade theorem.
orig:*stellar slices W*
+ *proj*:*stellar project slices I W* — We consider the projection of the system on I.
for *slices W I* + — An intact set is a set I satisfying the three assumptions below:
assumes *intact-wb*:$I \subseteq W$
and *q-avail*:*orig.quorum I* — I is a quorum in the original system.
and *q-inter*:$\bigwedge Q\ Q'\ .\ [\![proj.quorum\ Q;\ proj.quorum\ Q';\ Q \cap I \neq \{\};\ Q' \cap I \neq \{\}]\!] \Longrightarrow Q \cap Q' \cap I \neq \{\}$
— Any two sets that intersect I and that are quorums in the projected system intersect in I. Note that requiring that $Q \cap Q' \neq \{\}$ instead of $Q \cap Q' \cap I \neq \{\}$ would be equivalent.
begin

theorem *blocking-safe*: — A set that blocks an intact node contains an intact node. If this were not the case, quorum availability would trivially be violated.
fixes *S n*
assumes $n \in I$ **and** $\forall\ Sl \in slices\ n\ .Sl \cap S \neq \{\}$
shows $S \cap I \neq \{\}$
⟨*proof*⟩

theorem *cascade*:
— If U is a quorum of an intact node and S is a super-set of U, then either S includes all intact nodes or there is an intact node outside of S which is blocked by the intact members of S. This shows that, in SCP, once the intact members of a quorum accept a statement, a cascading effect occurs and all intact nodes eventually accept it regardless of what befouled and faulty nodes do.
fixes *U S*
assumes *orig.quorum U* **and** $U \cap I \neq \{\}$ **and** $U \subseteq S$
obtains $I \subseteq S \mid \exists\ n \in I - S\ .\ \forall\ Sl \in slices\ n\ .\ Sl \cap S \cap I \neq \{\}$
⟨*proof*⟩

end

2.4.2 The Union Theorem

Here we prove that the union of two intact sets that intersect is intact. This implies that maximal intact sets are disjoint.

locale *intersecting-intact* =
i1:*intact slices* W I_1 + *i2*:*intact slices* W I_2 — We fix two intersecting intact sets I_1 and I_2.
+ *proj*:*stellar project slices* $(I_1 \cup I_2)$ W — We consider the projection of the system on $I_1 \cup I_2$.
for *slices* W I_1 I_2 +
assumes *inter*:$I_1 \cap I_2 \neq \{\}$
begin

theorem *union-quorum*: *i1.orig.quorum* $(I_1 \cup I_2)$ — $I_1 \cup I_2$ is a quorum in the original system.
⟨*proof*⟩

theorem *union-quorum-intersection*:
assumes *proj.quorum* Q_1 **and** *proj.quorum* Q_2 **and** $Q_1 \cap (I_1 \cup I_2) \neq \{\}$ **and** $Q_2 \cap (I_1 \cup I_2) \neq \{\}$
shows $Q_1 \cap Q_2 \cap (I_1 \cup I_2) \neq \{\}$
— Any two sets that intersect $I_1 \cup I_2$ and that are quorums in the system projected on $I_1 \cup I_2$ intersect in $I_1 \cup I_2$.
⟨*proof*⟩

end

end

References

[1] E. Gafni, G. Losa, and D. Mazières. Stellar consensus by reduction. In *33nd International Symposium on Distributed Computing (DISC 2019)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019.