Please read this page first.

Here are my notes for the course on Byzantine failures (December 3, 2018).

What is important:
- The concept of Byzantine failure
- Safety proof, Liveness proof
- Proof by induction, proof by contradiction
- The first example (called "Simple example: n intermediary nodes")

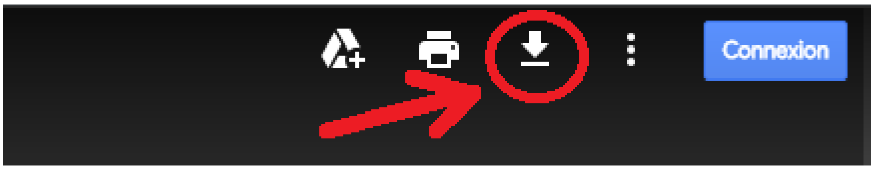
The next example ("General case: (2k+1)-connected graph") is "bonus", no need to memorize it. This is just to give you an example of "more complex proof" involving Byzantine failures.

You will find the end of the Safety proof (not finished during the course) in this document.
You can try to do the Liveness proof as an exercise if you want (a little bit long, but more straightforward).

About the exercise of the previous course ("Infinite grid"): this is also "bonus", but if you are interested, you can find the end of the solution here:

https://drive.google.com/file/d/1jM-KmP80M-0Sg3MmzegYq5U5BT1NvC_M/view?usp=sharing

(To download the pdf :)



B1

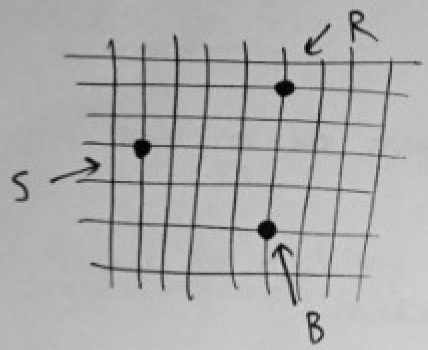
BYZANTINE FAILURES

1

CRASH failures : "dead" node

BYZANTINE failures : "evil" node

ILLUSTRATION :
BROADCAST ALGORITHM

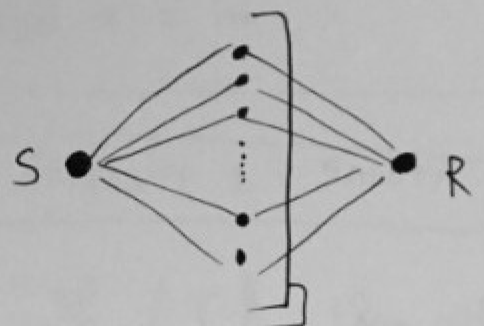


S : sender
R : receiver
B : BYZANTINE node

- S broadcasts (S, m)
- B broadcasts (S, m')
  $(m' \neq m)$
- R receives (S, m)
  AND (S, m')

→ what is the message of S ? m or m' ??

SIMPLE EXAMPLE : 2 "n intermediary nodes"



↳ n intermediary nodes

- S and R are correct
  (non-Byzantine)
- interm. nodes can be Byzantine
  → f = ~~[illegible]~~ max. number of Byzantine nodes
- S wants to send m to R
  ↑ message

ALGO

Preliminaries :

Define k :

Let k be such that n > 2k

$\boxed{B2}$ ($k+1$ = smallest number to have a majority among n)

- R has a set Ω (memory) and a variable x (initially $x = 0$)
- <u>GOAL</u> : to have $x = m$

<u>ALGO for S</u> :

- send m to neighbors

<u>ALGO for p</u> (any intermediary node):

- when receives m ~~fo~~ from p : send m to R

<u>ALGO for R</u> :

- when receives m from p : add (p, m) to Ω ($\Omega := \Omega \cup \{(p, m)\}$)
- when there exists $k+1$ nodes $\{p_1, \dots, p_{k+1}\}$ such that ....

.... $\forall i \in \{1, \dots, k+1\}$, $(p_i, m) \in \Omega$:

$x := m$

$\boxed{\text{PROPERTY 1 : SAFETY}}$

"If $f \leq k$, then either $x = 0$ or $x = m$"

nb. of BYZ. nodes

<u>PROOF</u> :

proof by contradiction

[SEEK]

suppose the opposite : $x = m'$ ($m' \neq m$)

$\rightarrow$ ATTA, there exists $k+1$ nodes $\{p_1, \dots, p_{k+1}\}$ such that, $\forall i \in \{1, \dots, k+1\}$, $(p_i, m') \in \Omega$

B3

for each node p_i :

ATTA: 2 possibilities :

(1) p_i received m' from S

(2) p_i is Byzantine

→ case (1) impossible

→ $\{p_1, \dots, p_{k+1}\}$ are Byzantine

→ we have $k+1$ Byzantine nodes : contradiction

(→ the result)

PROPERTY 2 : LIVENESS

"If $f \leq k$, we eventually have $x = m$"

PROOF:

Let $\{p_1, \dots, p_{k+1}\}$ be $k+1$ CORRECT (non-Byzantine) interm. nodes.

For each node p_i :

ATTA, p_i rec. m from S

→ p_i sends m to R

→ R rec. m from p_i and adds (p_i, m) to Ω

Eventually, we have:

$\forall i \in \{1, \dots, k+1\}$,

$(p_i, m) \in \Omega$

→ ATTA, $x = m$

PROP. 1+2 :

initially, $x = 0$,

and eventually, $x = m$

(we never have $x = m'$)

PROPERTY 3: OPTIMALITY

"If $f \geq k+1$, it is impossible to ensure ~~that we never~~ the safety property"

PROOF:

B4

let $\{p_1, \dots, p_{k+1}\}$
be $k+1$ <u>Byzantine</u> interm. nodes.

<u>possible situation:</u>

$\forall i \in \{1, \dots, k+1\}$,
p_i sends (p_i, m') to R

$m' \neq m$

$\rightarrow$ ATTA , $x = m'$
(no safety)

<u>CONCLUSION</u> :
we can tolerate
<u>at most</u> k Byz. failures

3

GENERAL CASE :
$(2k+1)$-connected graph

any graph:  ...

each node p has ...

- a message m_p to broadcast
- a set $p.R$ to store messages of other nodes
- a set $p.X$

<u>ALGO</u> for each node p :

- initially :
send $(p, \underbrace{\emptyset}_{\text{empty set}}, m_p)$ to neighbors

- when p receives (u, Ω, m) from a neighbor q, with $p \notin \Omega$ and $q \notin \Omega$:

(1) send $(u, \Omega \cup \{q\}, m)$ to neighbors

(2) add $(u, \Omega \cup \{q\}, m)$ to $p.X$
$(p.X := p.X \cup \{(u, \Omega \cup \{q\}, m)\})$

B5

- when there exists
a node q,
a message m,
and k+1 sets $(\Omega_1, \dots, \Omega_{k+1})$
such that

$$\underbrace{\bigcap_{i=1}^{i=k+1} \Omega_i}_{\Omega_1 \cap \Omega_2 \cap \dots \cap \Omega_{k+1}} = \{q\}$$

AND

$\forall i \in \{1, \dots, k+1\}$,
$(q, \Omega_i, m) \in p.X$

$\rightarrow$ add (q, m) to $p.R$

HYPOTHESES:

- at most k Byzantine nodes
- graph $(2k+1)$-connected

$\boxed{\text{PROPERTY 1 : SAFETY}}$

"Let p and q be 2 correct nodes;
we never have $(p, m) \in q.R$ with $m \neq m_p$"

(i.e. no "false" message accepted)

PROOF:

proof by contradiction

suppose the opposite:
"there exists 2 correct nodes p and q such that
$(p, m) \in q.R$ with $m \neq m_p$"

$\rightarrow$ ATTA, there exists k+1 disjoint sets
$(\Omega_1, \dots, \Omega_{k+1})$
such that

$$\bigcap_{i=1}^{i=k+1} \Omega_i = \{p\}$$

AND

$\forall i \in \{1, \dots, k+1\}$,
$(p, \Omega_i, m) \in q.X$

$\boxed{\text{SUB-PROPERTY :}}$

"each set Ω_i contains a Byzantine node"

$\boxed{B6}$

→ proof by contradiction

suppose the opposite:

"Ω_i contains <u>no</u> Byzantine node" (all correct)

$$N = |\Omega_i|$$

$\mathcal{P}_j$: " there exists a node $p_j \in \Omega_i$ such that p_j sent $(p, \Omega_i - \{p_j, \dots, p_1\}, m)$"

→ proof by induction

(1) $\mathcal{P}_1$:

as $(p, \Omega_i, m) \in q.X$,

ATTA,

q rec. $(p, \Omega_i - \{p_1\}, m)$

from a node $p_1 \in \Omega_i$

→ p_1 sent $(p, \Omega_i - \{p_1\}, m)$

→ $\mathcal{P}_1$ true

(2) suppose $\mathcal{P}_j$ true

$(j \in \{1, \dots, N-1\})$

→ ATTA

p_j received $- \{p_{j+1}\}$

$(p, \Omega_i - \{p_j, \dots, p_1\}, m)$

from $p_{j+1} \in \Omega_i - \{p_j, \dots, p_1\}$

→ p_{j+1} sent

$(p, \Omega_i - \{p_{j+1}, \dots, p_1\}, m)$

→ $\mathcal{P}_{j+1}$ true

(3) $\mathcal{P}_N$ true :

$p_N \in \Omega_i$ sent

$$(p, \underbrace{\Omega_i - \{p_N, \dots, p_1\}}_{= \emptyset\ !}, m)$$

→ 2 possibilities :

(A) $p_N = p$ → impossible as $m \neq m_p$

<u>OR</u>

(B) p_N is <u>Byzantine</u> !

(end of sub-property)

$\boxed{B7}$

- each set Ω_i contains a Byzantine node
- $k+1$ sets "Ω_i"

$\rightarrow$ as $\bigcap_{i=1}^{i=k+1} \Omega_i = \{\underbrace{p}_{\text{correct}}\}$:

there are at least $k+1$ Byzantine nodes

$\rightarrow$ impossible $\rightarrow$ the result