11-5-2019

① EIG Stop.

Byzantine Failures.

Behavior of a faulty process: any arbitrary behavior and in particular, all faulty processes can collude among themselves.

Messages with authentication (digital signatures) - easier to solve.
No digital signatures for messages.

We need $n > 3f$ processes for consensus despite Byzantine faults without message authentication.

f = # of faulty processes.
Need n = min of $3f+1$

→ Argue that $f=1$, $n=3$, no solution to agreement Problem.

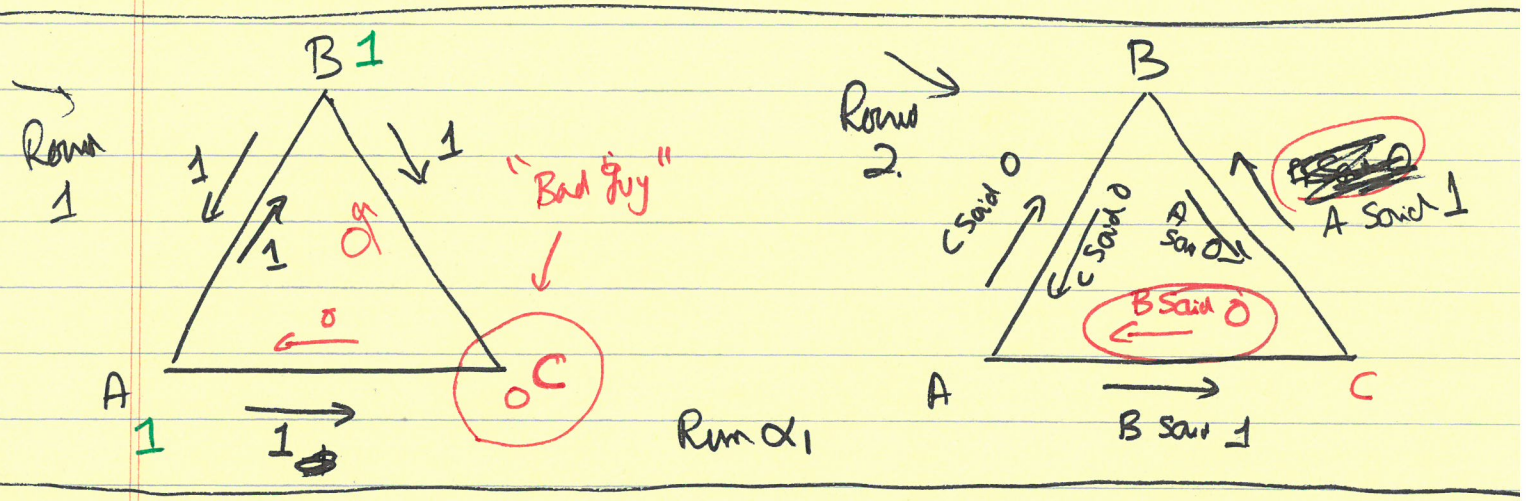
1. Termination -
2. Validity: If all non-faulty processes start with $v \in V$ as the input value, then v is the only possible solution.

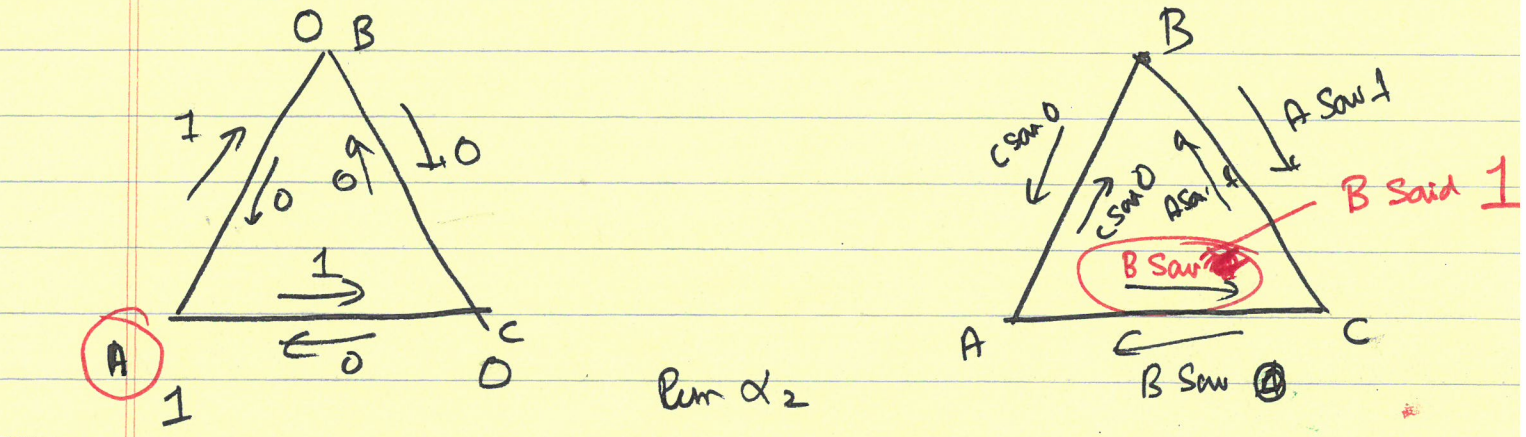
Agreement 3. No two non-faulty processes decide on different values.

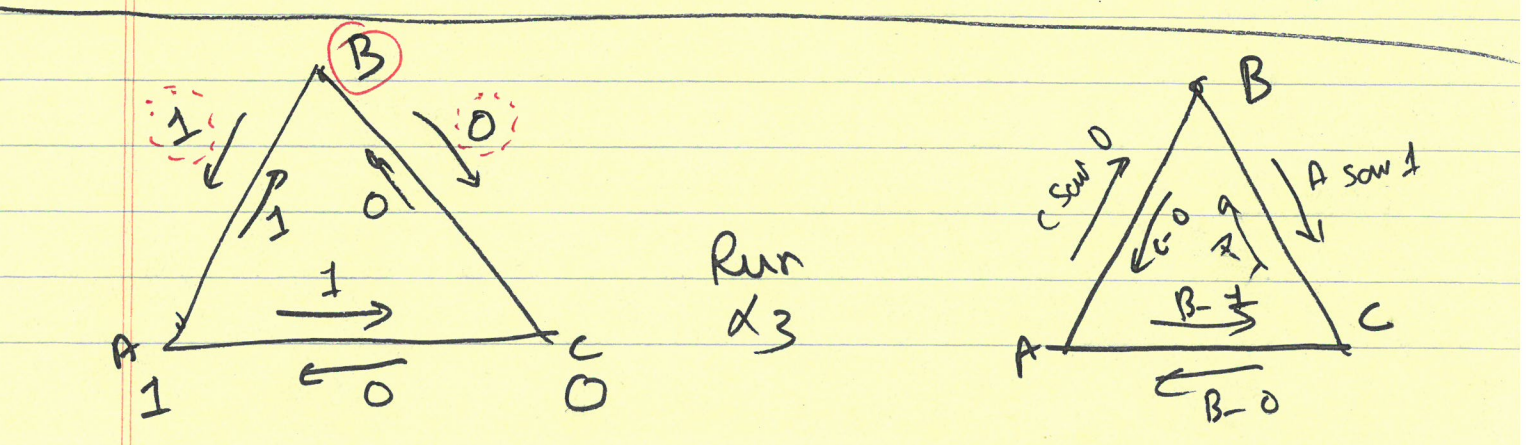
(2) The algorithms are of the form:

Round 1: Send local value to all.
Receive -- -- s from others.

Round #>1: Record received values.
send received values to others







(3) $\alpha_1 \overset{A}{\sim} \alpha_3$: From A's point of view α_1 & α_3 are indistinguishable

$\alpha_2 \underset{C}{\sim} \alpha_3$: From C's point of view, α_2 & α_3 are identical.

A decides on 1 in α_1 [Both non-faulty processes start with 1]
(validity condition)

C decides on 0 in α_2.

in α_3, C decides on 0 [α_2 & α_3 are same from C]

in α_3, A decides on 1 (α_1, α_3 are same for A)

$\Rightarrow$ agreement is violated

$f=1$, $n=3$ ~~so~~ no solution.

$f>1$? Can show via simulation of >1 faulty process case.

$n = \min 3f+1$ for consensus.

EIG Byz Algorithm

Run for $f+1$ rounds (like in EIG STOP) and propagate {val} values with labels.

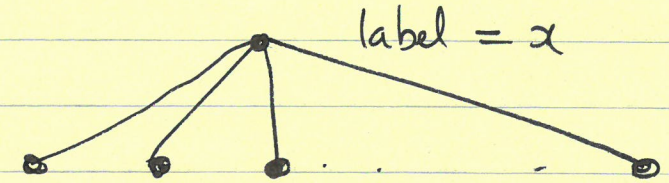
Every node of the EIG tree has label and val.

Associate another # to each node of the EIG tree in addition to val.

newval ( ):

leaf — newval(x) = val(x) if x is a label of a leaf vertex

Interior vertex



newval(x) = strict majority of the newval of its children if strict majority exists
else = v_0, default value.

All processes agree on what the new val is. before the algorithm starts.