11-7-2019

① EIG BYZ algorithm

Correctness:

Lemma 6.15 After $f+1$ rounds: if ~~...~~ i, j & k are non-faulty processes, $i \neq j$, then $val(x)_i = Val(x)_j$ for every label x ending in k

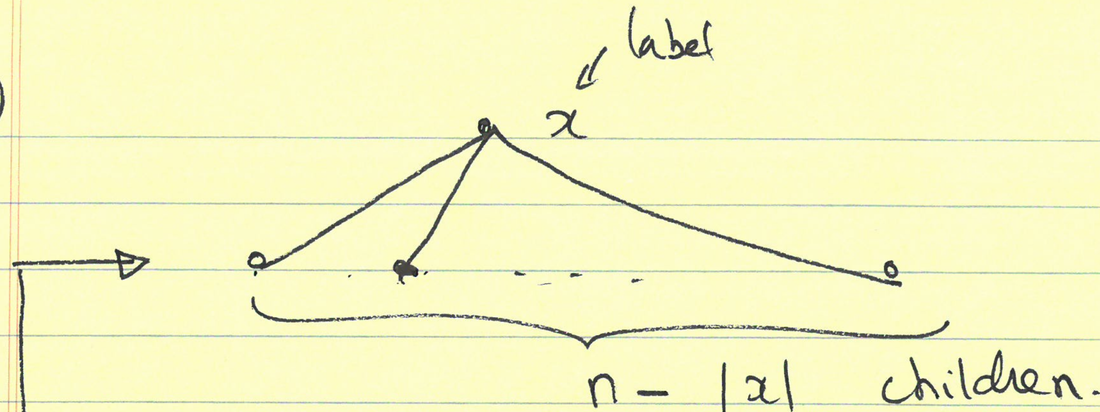
Proof: Fairly straightforward (Since k is non-faulty, it sends $(\ldots k, v)$ to both i & j
...

Lemma 6.16 Let x be a label ending in non-faulty process's id [$x = \ldots k$; k is non-faulty].
There exists $v \in V$ such that
$val(x)_i = newval(x)_i = v$ for all non-faulty i.

Proof By induction from leaf & going up in the EIG tree.

Basis: Leaf: True by Lemma 6.15 ✓

Induction Step: Suppose $|x| = r$; $1 \leq r \leq f$
($r = f+1$, ok by basis)
All non-faulty processes have
Same $Val(x)_l = v$ at process l.
$val(xl) = v$ (if l is non-faulty)
at all non-faulty processes.



Among these vertices, any node label ending with non-faulty process id will have same val (among all non-faulty processes).

By induction hypothesis, all these nodes have same $val(xl) = \cancel{val} \; newval(xl) = v$ if l is non-faulty process's id.

Among the children of x, a strict majority exists. $n > 3f$; $|x| \le f$

$$n - x > 2f$$

Thus $newval(x)_i = newval(x)_j = v \;\; \forall$ i, j, l all non-faulty, x ending in non-faulty.

<u>Validity:</u> ✓ exercise. (Lemma 6.17)

<u>Termination.</u> ✓ (f+1 rounds)

<u>Agreement:</u> 2 Definitions

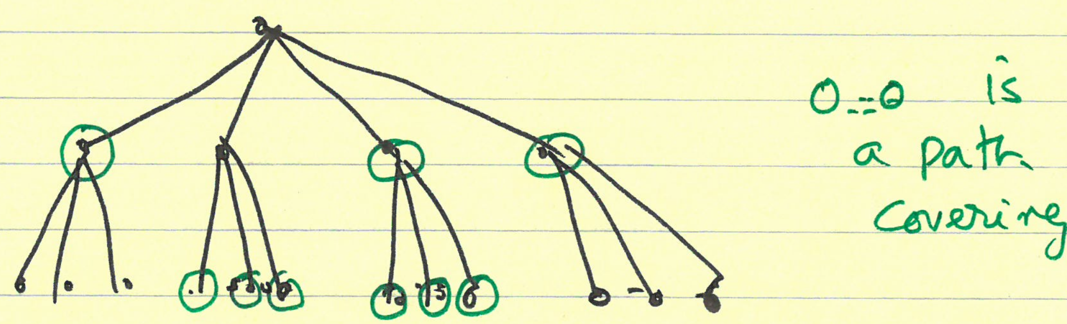
③

(a) Common node of EIG tree.

• x is label.

if newval(x) is same at all non-faulty processes, node x is <u>common</u>

(b) Path covering: C A subset of nodes of the EIG Tree is a path covering if every path from every leaf of EIG tree to the root includes at least one member of C.

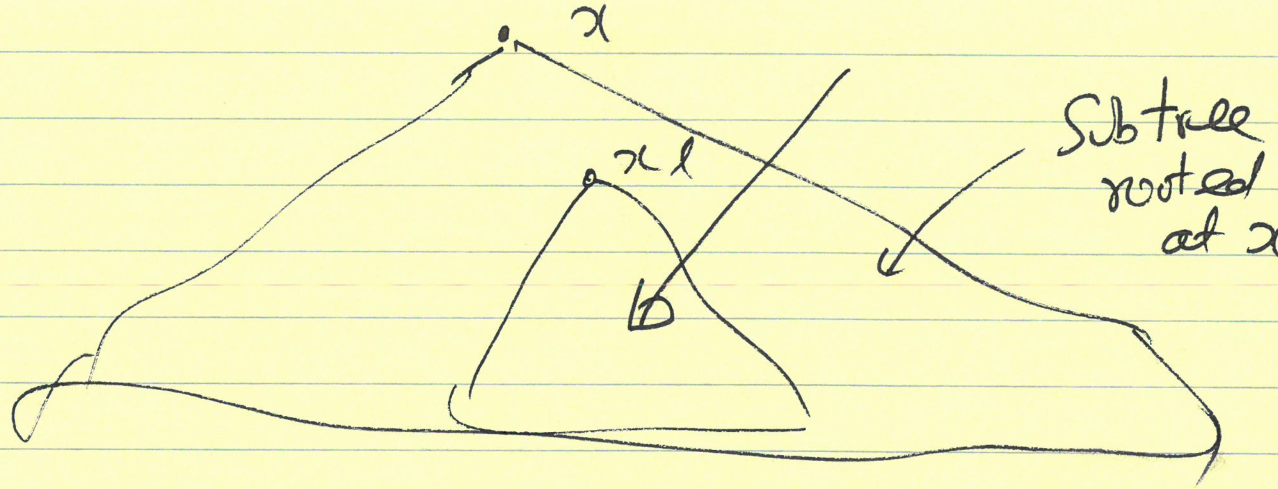


<u>Lemma 6.18</u>: After $f+1$ rounds, there exists a path covering that is common.

Trivial Proof

<u>Lemma 6.19</u>: After $f+1$ rounds, the following holds: x is a label of EIG tree. If there exists a common path covering of the subtree rooted at x then x is common.

(4)



Proof by induction (Leaf, going up the tree)

Basis is obvious

Induction step $|x| = r$: $0 \le r \le f$

There exists a common path covering of subtree rooted at x.
(Let C = common path covering of x's subtree rooted at x).
if $x \in C$: we are done.

else { Consider all children of x of the form xl.
C induces a ~~path~~ common path covering of subtree rooted at xl.
All children of x are common. (induction hypothesis)
$\Rightarrow$ newval(x) is based on ~~that~~ newval of x's non-faulty children.
val(x) is common [All apply same ~~rep~~ majority]

(5) Lemma 6-20: Root λ is common.
follows from previous Lemmas.

$\Rightarrow$ Agreement ✓
$n > 3f$ needed.

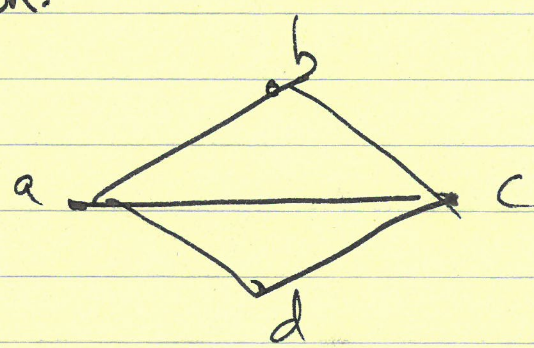
Graph Not completely connected ?

Need other conditions

Faulty processes may drop all messages to be forwarded!

Connectivity of a Graph G.

Conn(G) = min # of nodes whose removal results in G being disconnected or results in 1-node graph.



Menger's Theorem: Conn(G) = c if and only if # of node disjoint paths between every pair of vertices is $\geq c$.

5

Process i decides on renewal (λ).

<u>Example</u>

$f = 1$ $\quad n = 4$ (or higher)

(6) <u>Theorem 6.29</u> : Consensus despite Byzantine failures is possible if and only if these 2 hold.

$n > 3f$

$Conn(G) > 2f$

<u>Quiz 4 material</u> : After AsynchGHS.

Synchronizer

Consensus despite process failures

- Fail stop
- Byzantine

1pm – 2pm : office hours on

Sunday, Nov 10, 2019