Distributed Byzantine Computation

7/7/2021
Lecture 13
Scribe: Avi Cohen

Byzantine node taken over by some bad adversary

- drop messages.
- random messages
- as bad as one can imagine.

A node that is not Byzantine is called correct.

f - number of Byzantine nodes.

[LPS, Dolev '80]:

Computation is possible only if: $f < \min\left\{ \frac{\text{vertex-conn. of graph}}{2}, \frac{n}{3} \right\}$

Graph G has vertex-conn. X if $\forall u,v \in G$ are connected by $\geq X$ vertex-disjoint paths.

Byzantine Agreement

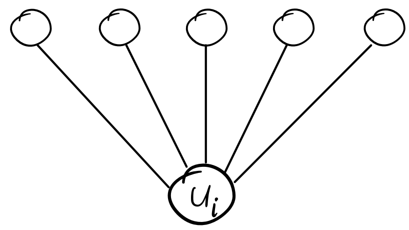
- n-vertex complete graph.
- $f < \frac{n}{3}$ Byzantine nodes.
- Every u_i has initial value $x_i \in \{0,1\}$

Agreement: all correct nodes should output the same bit.

Validity: If all correct nodes have the same x_i values then this should be the output.

The King Algorithm

- all IDs in [1,n]



For node u_i Let x be the original value of u_i.

For $p=1$ to $f+1$ do:

R_1 Broadcast val(x) to all nodes.

R_2
- If received val(y) from $\geq n-f$ nodes
  Broadcast propose(y).
- If received propose(w) from $\geq f+1$ nodes
  $x \leftarrow w$.

R_3
u_p is the king of the phase.

Case $u_i = u_p$: broadcast current value w to everyone.

Case $u_i \neq u_p$: If propose(x) was received from $\leq n-f-1$ nodes:
$x \leftarrow$ king's value (w).

Lemma 1: validity holds.

Pf: Say all correct nodes have $x_i = 0$.

Then get val(0) from $\geq n-f$ nodes

propose " " "

The value is kept since if-cond. of R_3 does not hold. $\square$

Lemma 2: all correct nodes that propose in R_2, propose the same value.

Pf: u, v correct nodes, u propose(x) and v sends propose(y). Assume $x \neq y$.

- u received $x \geq n-f$ nodes $\geq n-2f$ correct nodes.
- v " y " " " " ".

\# correct nodes $\geq n-2f+n-2f = 2n-4f$

\# nodes $\geq 2n-3f > n$, contradiction. $\square$

Cor: If $\exists u$ receiving propose(x) from $\geq f-1$ nodes &

$\exists v$ " " y " " "

$\Rightarrow x = y$.

Proof: $\exists$ correct node w sending propose(x).

$\exists$ correct node w' sending propose(y).

By Lemma 2, $x = y$.

Lemma 3: Let p be a phase of a correct king, then at the end of the phase, all nodes get the king's value and maintain this value.

Proof:

Case 1: If-cond of R_3 holds. √

Case 2: $\exists u$ for which the If-cond. does not hold.

Let x be the current value of u.

u received propose$(x) \geq n-f$ nodes

$\geq n-2f$ correct nodes.

$\Rightarrow$ king got propose$(x) \geq n-2f \geq f+1$ nodes.

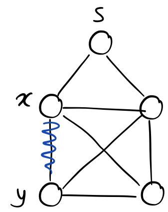
$\Rightarrow$ king value $= x$. $\square$

Complexity: $O(f)$ rounds.

What can we do if the graph is not a clique?

Byzantine Broadcast for General Graphs

- Byzantine edges. (Single Byzantine edge e')

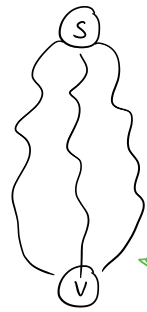


Adversarial Congest Model:

- 3 edge connected graph.
- In every round exchange $O(\log n)$-bit with neighbors.
- Messages through $e' = (x,y)$ are corrupted.
- The adversary knows everything.

<u>Goal</u>: Given source s holding message m_0,

all nodes should output m_0.



Can simply take majority over the paths from s to v. (Naive and Costly Solution).

<u>Today</u>: $\tilde{O}(D^3)$-round alg.

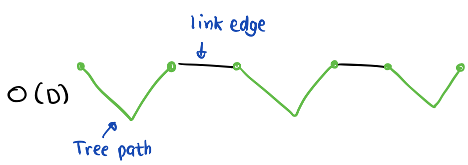
* for simplicity assume all nodes know D (or $O(1)$-approximation).

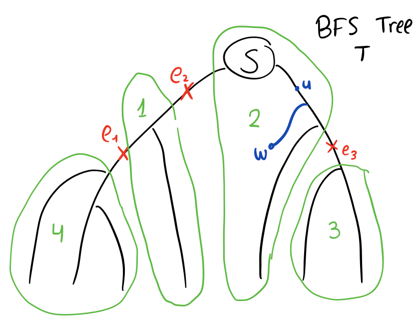
<u>Obs</u>: For every $(f+1)$-edge connected graph G with diam D,

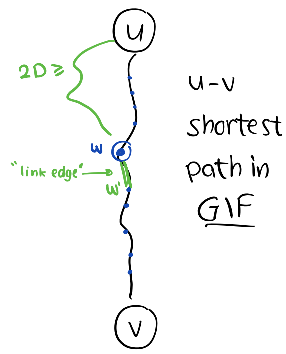
it holds that $\mathrm{Diam}(G \setminus F) = O(f \cdot D)$ for every $F \subseteq E$, $|F| \leq f$.

<u>Proof</u>: u, v, $F \subseteq E$, $|F| \leq f$, show $d(u,v,G\setminus F) = O(f \cdot D)$.

$\#$ comp in $T \setminus F \leq |f| + 1$.







$\Rightarrow O(fD)$ length.

The observation implies that there is always a path of "reasonable" length ignoring the Byzantine edge e'. So there is hope!

Covering family of a D-diameter graph G is an ordered set

$$\mathcal{G} = \{G_1, \ldots, G_\ell\}$$

where $G_i \subseteq G$ and $\ell = \tilde{O}(D^2)$.

For every edge $e \in G$, and $\forall$path $P \subseteq G \setminus e$ of length at most $c \cdot D$,

there exists $G_i \in \mathcal{G}$ s.t.:

1) $P \subseteq G_i$

2) $e \notin G_i$

<u>Example:</u> (Randomized Construction)

$$G_i = G[p] \qquad p = 1 - \frac{1}{cD}$$

$$\Pr(G_i \text{ covers } P \cdot e) = \underbrace{\left(1 - \frac{1}{cD}\right)^{|P|}}_{\text{Taking all edges of path } P} \cdot \underbrace{\frac{1}{cD}}_{\text{Not taking the edge } e} \geqslant \left(1 - \frac{1}{cD}\right)^{cD} \frac{1}{cD} \approx \frac{1}{e} \cdot \frac{1}{cD}$$

A covering family $\mathcal{G}$ is **locally known** if given index i, and (u,v),

v knows if $(u,v) \in G_i$.

Byzantine Broadcast with Single Byzantine Edge

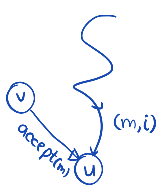
<u>Phase 1:</u> Flood (m, i) messages on every subgraph $G_i \in \mathcal{G}$ for $O(D)$ rounds.

<u>Phase 2:</u> s sends accept(m_0) to neighbors

<u>For $O(D)$ rounds do:</u>

Node u upon receiving accept(m) from v:

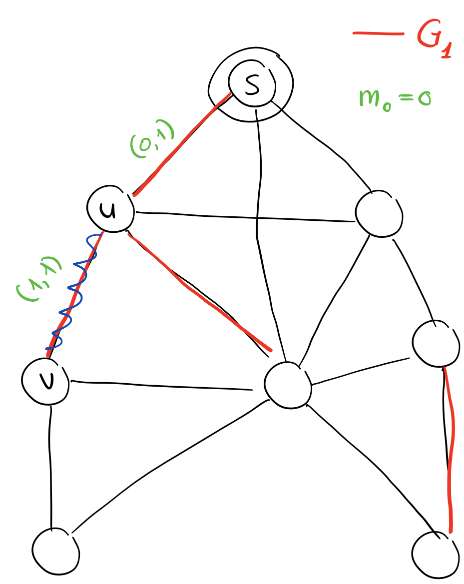
will accept m only if:



- received (m, i) s.t. $(u,v) \notin G_i$

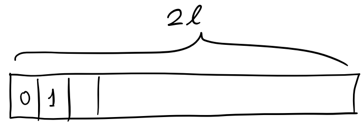
- Send accept(m) to neighbors

(G is locally known)



Phase 1 can be implemented in $\tilde{O}(D^3)$ rounds.

- Run in steps of $2\ell = \tilde{O}(D^2)$ rounds

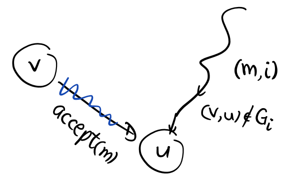


Or even better: just work subgraph by subgraph for $O(D)$ rounds.

Lemma 1: No node accepts the wrong message.

Let u be the first node accepting wrong message (by round number)

$\Rightarrow$ (m,i) is received for G_i s.t. $(v,u) \notin G_i$ $\Rightarrow$ contradiction.



Obs: s-u path $P \subseteq G \setminus e'$ of length $\leq c \cdot D$

and let G_i be s.t. $P \subseteq G_i$,

then u receives (m_0, i).

Lemma: all nodes accept.

Pf: By induction on the distance from s in $G' \setminus e'$

Claim: by round r, all nodes at distance $\leq r$ from s in $G \setminus e'$ accept.

consider a node v at distance $r+1$.

- Since the graph is 3-edge connected, there is an s-v path P in $G \setminus \{(u,v), e\}$ and $|P| = O(D)$.
- By covering property, $\exists G_i$ s.t. $P \subseteq G_i$, $(u,v) \notin G_i$
- By the obs, v received the message (m_0, i)

$\Rightarrow$ accepts m_0. $\square$