Local verification of global proofs

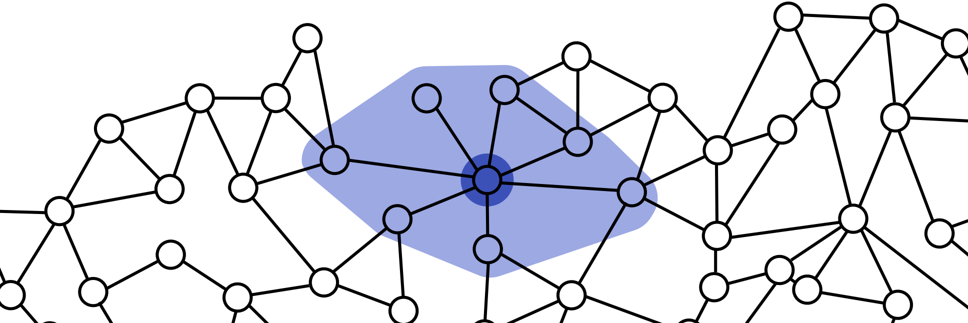
Laurent Feuilloley (SU)

joint work with
Juho Hirvonen (Aalto)

ESTATE+DESCARTES meeting · April 2019

Local decision

- Setting : distributed synchronous network computing.
- Goal : check whether the network satisfies some property.
- Constraint : every node knows only its view at distance 1.
- Identifiers on $O(\log n)$ bits.

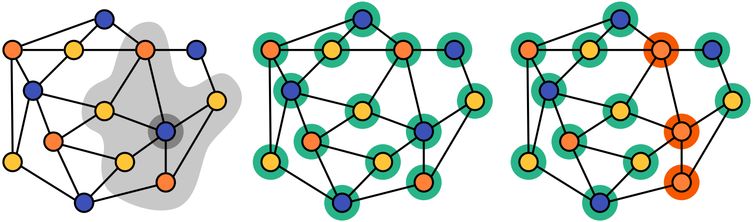


Decision rule

[Awerbuch, Patt-Shamir, Varghese 91], [Naor,Stockmeyer 93], [Itkis, Levin 94], [Afek, Kutten,Yung 97].

Decision rule :

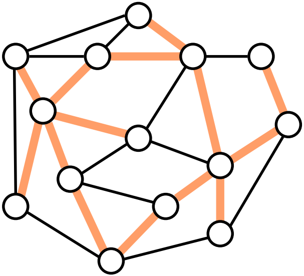
- Every node makes one (local) decision : *accept* or *reject*.
- The configuration is accepted if and only if all the local decisions are *accept*.



Limits of local decision

Property to check :
The marked edges form a spanning tree of the network.

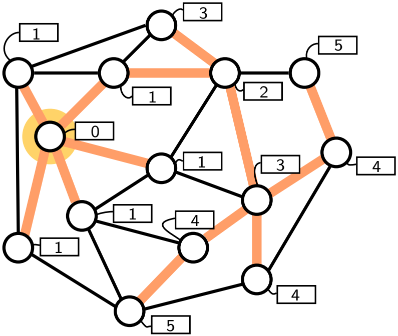
Theorem [Folklore] :
There is no local decision algorithm to decide this property.



Extra information

Idea from fault-tolerance : store extra information at the nodes.

Example : for spanning trees, store root ID, and distance to root.



Local certification

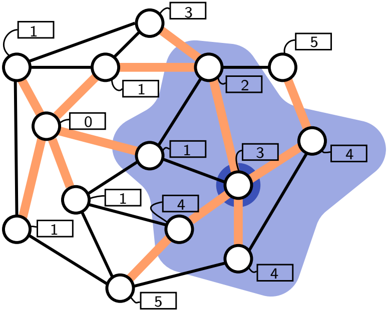
Abstraction :
Certificates are given by a prover, and the nodes verify.

Definition [Korman-Kutten-Peleg 05] :
A certificate (or proof) assignment is a function $V \to \{0,1\}^k$.
(k is the size.)

Correctness rule :

- Good configuration $\to \exists$ certificates, $\forall v$, v accepts.
- Bad configuration, $\to \forall$ certificates, $\exists v$, v rejects.

Spanning tree scheme

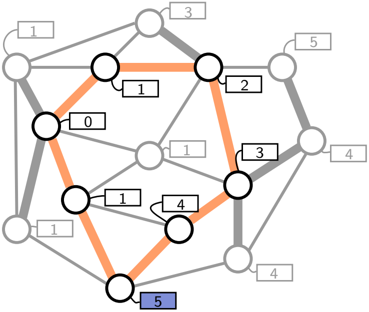


Verifier on node v :

- Check : neighbours have same root-ID.
- If $d = 0$:
  check the root-ID
  $\forall$ neighbour u, $d(u) = 1$.
- If $d > 0$:
  $\exists$ neighbour u, $d(u) = d - 1$
  $\forall$ neighbour $w \neq u$,
  $d(w) = d + 1$

Theorem [Itkis-Levin 94] : The spanning tree scheme is a correct.

Spanning tree scheme



Verifier on node v :

- Check : neighbours have same root-ID.
- If $d = 0$:
  check the root-ID
  $\forall$ neighbour u, $d(u) = 1$.
- If $d > 0$:
  $\exists$ neighbour u, $d(u) = d - 1$
  $\forall$ neighbour $w \neq u$,
  $d(w) = d + 1$

Theorem [Itkis-Levin 94] : The spanning tree scheme is a correct.

Uniformity

In the spanning tree scheme, we have *two parts* :

1. The ID of the root. Uniform (the same for every node).
   $\hookrightarrow$ "global".
2. The distance to the root. Different for every node.
   $\hookrightarrow$ "local".

Uniformity

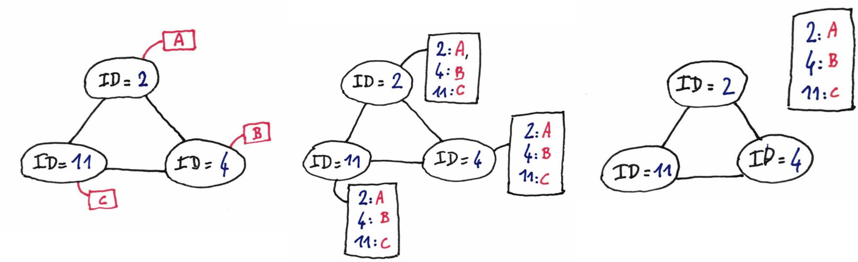
Questions : what if we want to have the whole proof uniform ?
Is it always possible ? At what price ?

Why should we care ? Study of locality. Other models.

First elements : For some properties, the best proofs are uniform.
$\rightarrow$ Isomorphism, AMOS.

General transformation

Non-uniform $\rightarrow$ **uniform** : list everything with the ID.



Size : $k \rightarrow O(n \cdot (\log n + k))$ $\rightsquigarrow$ Can we do better ? ?

For spanning trees

Size : $k = \log n \rightarrow O(n \cdot (\log n + k)) = O(n \log n)$.

$\rightsquigarrow$ Can we do better than $O(n \log n)$?

Remark :
The ID part is uniform from the start, the problem is the distances.

Answer : nope.

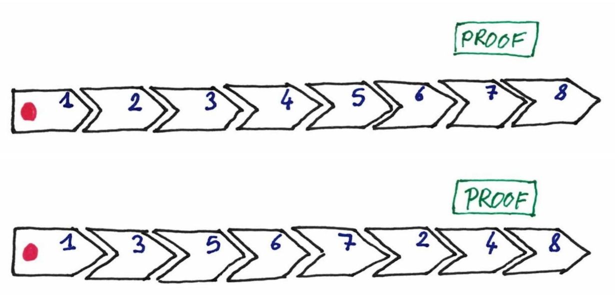
Proof (or some bits of it) :

Somehow :
certify a spanning tree $\sim$ certify that there is exactly one root.

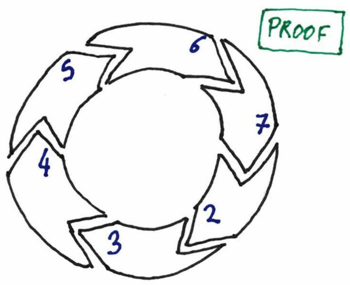
Previous works :
At most one root needs local $\Omega(\log n)$.

This work
At least one root needs global $\Omega(n \log n)$.

Proof



Proof



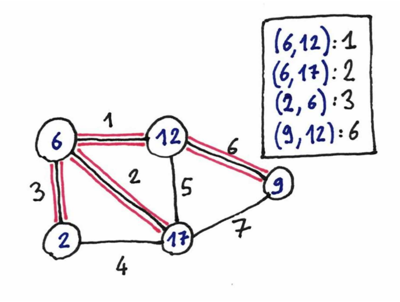
Lemma :
not two permutations of blocks can have the same global proof.

Nb of permutations $= n! \Rightarrow$ at least $n!$ different proofs.
$\hookrightarrow$ we need $\log(n!)$ bits, that is $\Omega(n \log n)$.

Minimum spanning tree

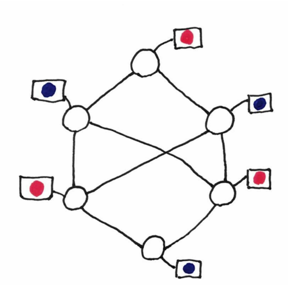
Local size : $\Theta(\log^2 n)$.

General transformation :
$k = \log^2 n \rightarrow O(n \cdot (\log n + \log^2 n)) = O(n \log^2 n)$.
We can do better ! We can shave a log.
Same space as for simple spanning trees : $O(\log n)$.



Open question

Property to check : bipartiteness.
Local size : $O(1)$ bits.
General transformation : $O(n \cdot (\log n + 1)) = O(n \log n)$.



Can we do better ? ?