# Distributed Interactive Proofs

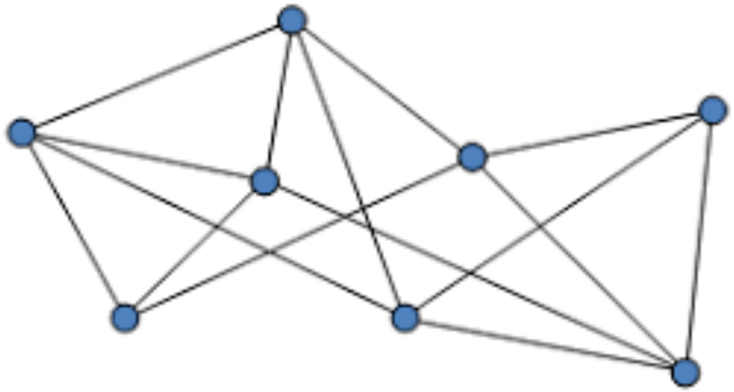
Pierre Fraigniaud

Joint work with Pierluigi Crescenzi and Ami Paz

Workshop QuData, Paris, February 20-21, 2019

# Decision Problems

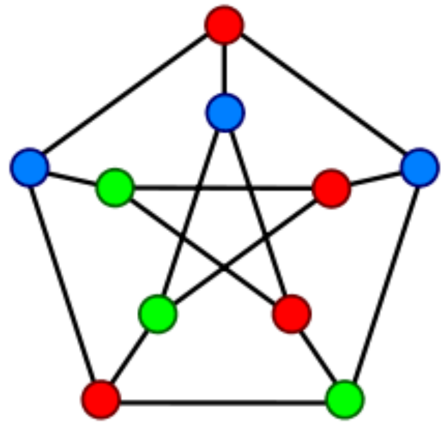
[NS, 1995]



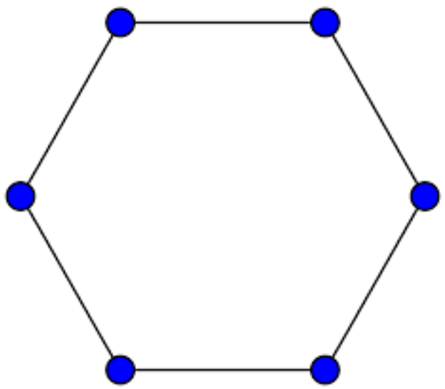
- Network computing
- Boolean predicate on labeled graphs:
  - c is a proper coloring
  - T is a (minimum-weight) spanning tree

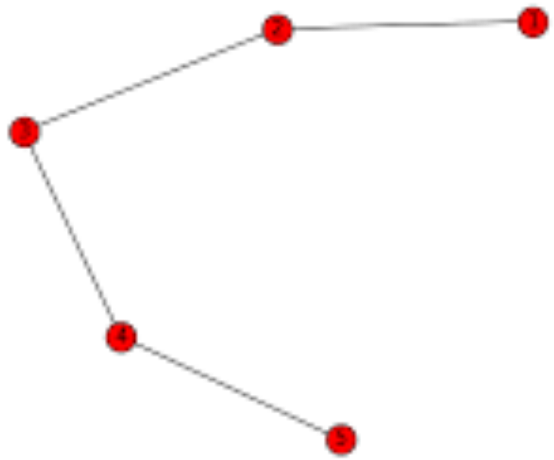
Predicate is satisfied ⟺ all nodes accept

# Examples



- c is a proper coloring $\in$ LD
- G is 3-colorable $\notin$ LD
- G is acyclic $\notin$ LD



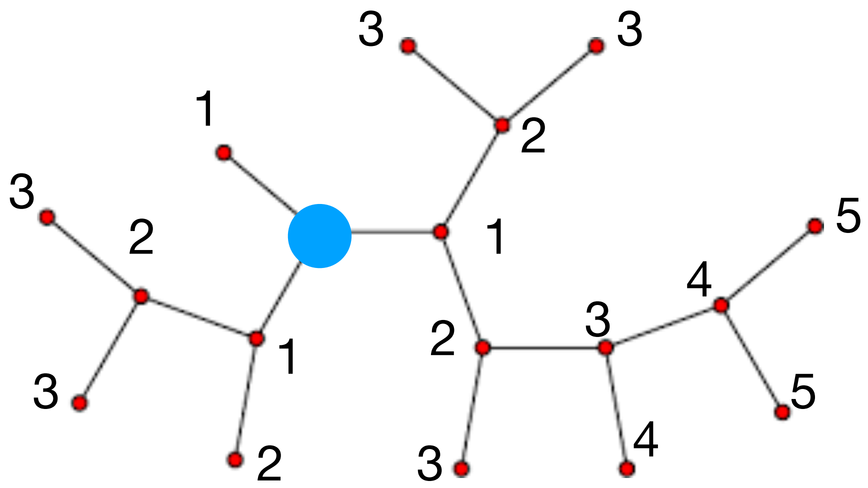


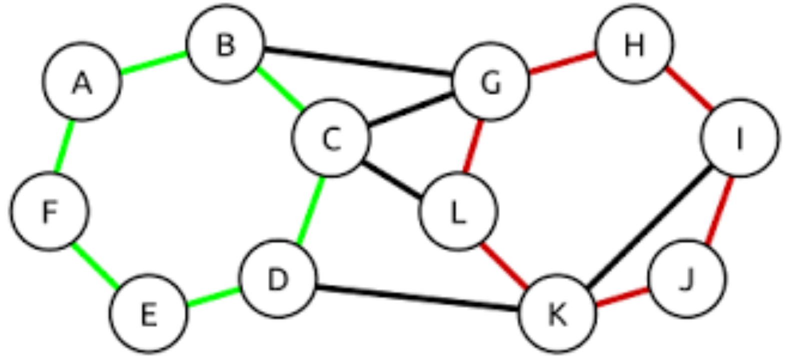
# Locally Checkable Proofs

[GS, 2016]

- Variants:
    - Proof-Labeling Schemes [KKP, 2010]
    - Non-Deterministic Local Computing [FKP, 2013]

- G is acyclic $\in \Sigma_1$LD(log n)



# The class $\Sigma_1$LD

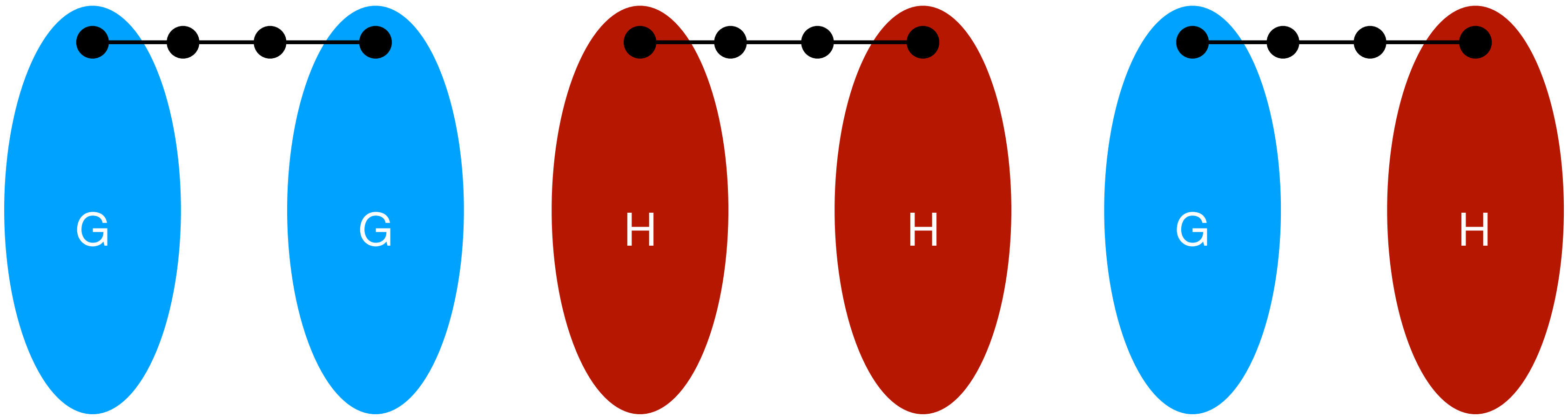
- Configuration = (G,x,id) where $x: V(G) \to \{0,1\}^*$
- Distributed language = set of configurations
- LD = {locally decidable languages}
- $L \in \Sigma_1$LD if and only if there exists a local algorithm s.t. for every (G,x,id)

$$(G,x,id) \in L \Leftrightarrow \exists\, y: V(G) \to \{0,1\}^* : \text{all nodes accept}$$

- Application to distributed fault-tolerant algorithms

# Size of certificates

- All languages are in $\Sigma_1 LD(n^2)$ — every node is provided with the complete description of the network
- Non 3-colorability requires $\Omega(n^2)$-bit certificates
- Symmetry requires $\Omega(n^2)$-bit certificates



# Local Hierarchy

[FFH, 2016]

- Non 3-colorability $\in \Pi_2 LD(\log n)$

$$(G,x,id) \in \neg 3col$$

$$\Updownarrow$$

$$\forall\, y_1\; V(G) \rightarrow \{0,1\}^* \;\; \exists\, y_2 : V(G) \rightarrow \{0,1\}^* : \text{all nodes accept}$$

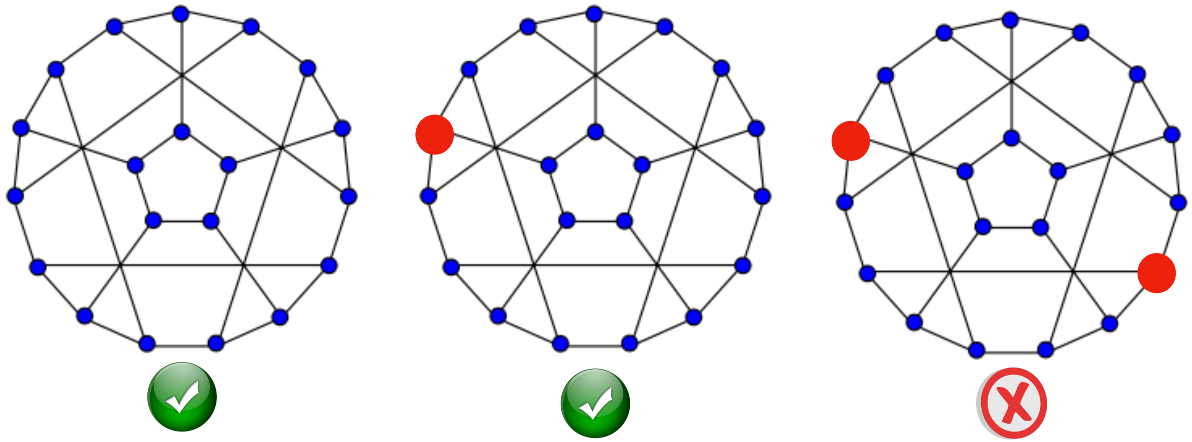
  - $y_1$ interpreted as a 3-coloring ($O(1)$ bits)
  - $y_2$ encodes a spanning tree pointing to an error ($O(\log n)$)

- Many optimization problems are in $\Sigma_3 LD(\log n)$

# Randomized Protocols

[FKP, 2013]

- At most one selected (AMOS)

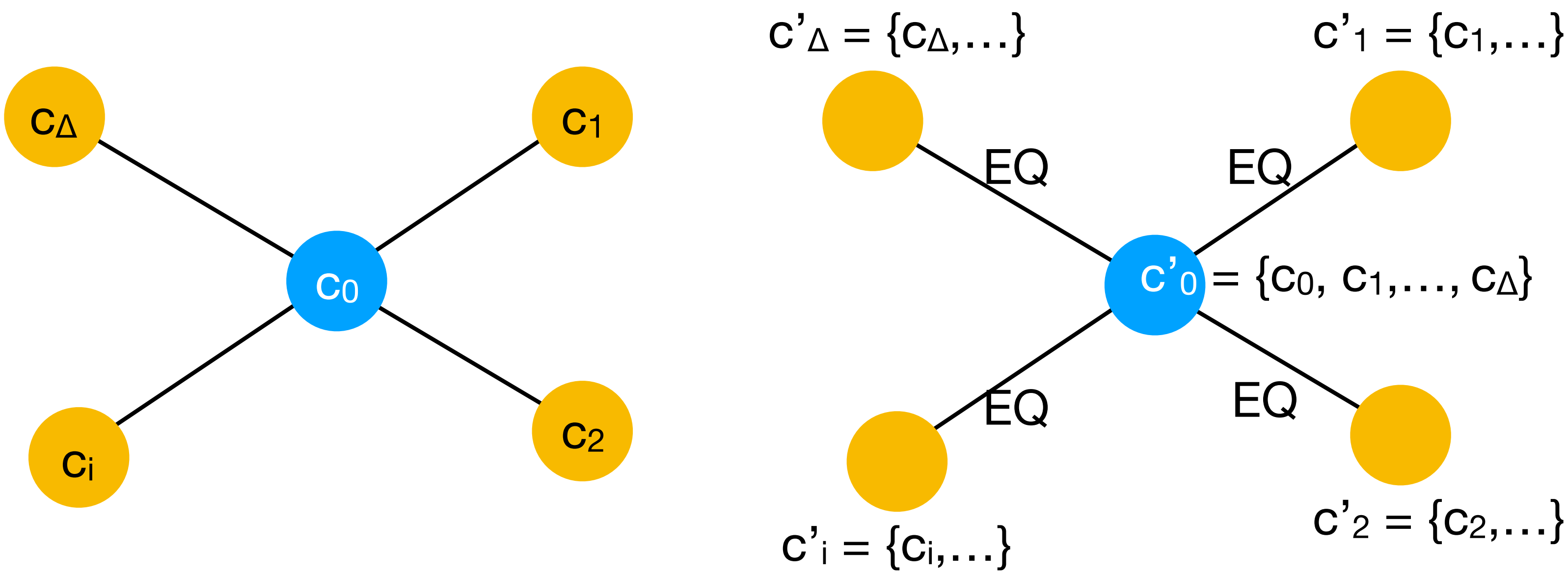


- Decision algorithm (2-sided):
  - let p = $(\sqrt{5}-1)/2 = 0.61\ldots$
  - If not selected then accept
  - If selected then accept w/ prob p, and reject w/ prob 1-p

- Issue with boosting! — But OK for 1-sided error

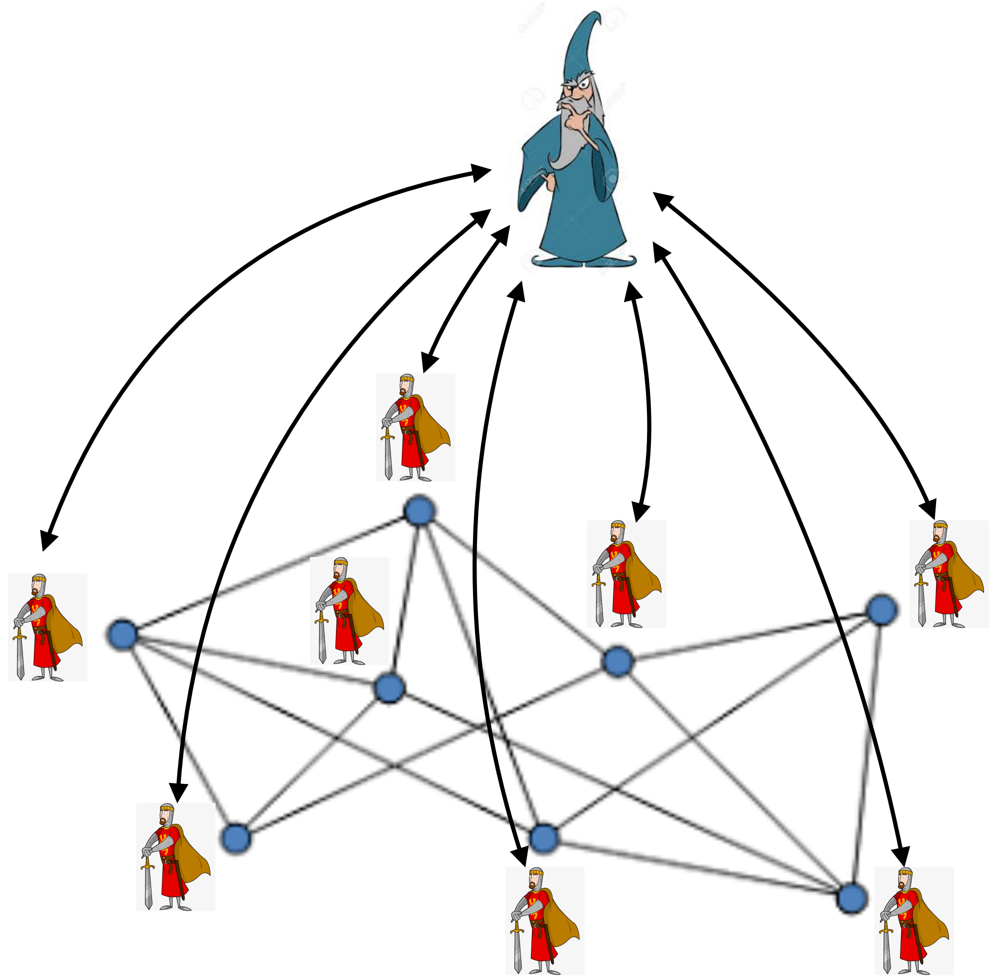
# Randomized Proof-Labeling Scheme [BFPS, 2015]

- Proof-Labeling scheme (or locally checkable proof) in which the verifier is randomized
- If L has a PLS with certificates of size k then L has a RPLS with certificates of size O(Δk) but with communication complexity O(log k)



# Distributed Interactive Protocols

[KOS, 2018]

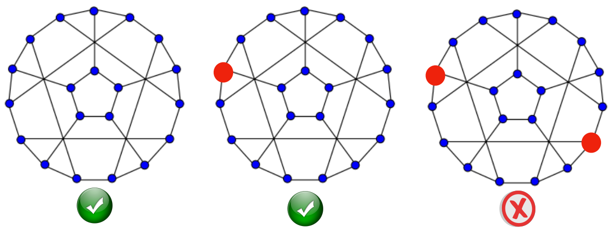


- Arthur-Merlin Phase *(no communication, only interactions)*
- Verification Phase *(only communications)*

- Merlin has infinite communication power
- Arthur is randomized

- k = #interactions
- dAM[k] or dMA[k]

# Example: AMOS



- In BPLD with success prob $(\sqrt{5}-1)/2 = 0.61\ldots$
- In $\Sigma_1$LD(O(log n)) — Not in $\Sigma_1$LD(o(log n))
- Not in dMA(o(log n)) for success prob > 4/5
- In dAM(k) with k random bits, and success prob $1-1/2^k$
  - Arthur independently picks a k-bit index at each node u.a.r.
  - Merlin answer $\perp$ if no nodes selected, or the index of the selected node

# Sequential setting

- For every $k \geq 2$, $AM[k] = AM$
- $MA \subseteq AM$ because $MA \subseteq MAM = AM[3] = AM$
- $MA \in \Sigma_2 P \cap \Pi_2 P$
- $AM \in \Pi_2 P$
- $AM[poly(n)] = IP = PSPACE$

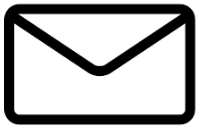
# Known results

[KOS 2018, NPY 2018]

- Sym $\in$ dAM($n \log n$)
- Sym $\in$ dMAM($\log n$)
- Any dAM protocol for Sym requires $\Omega(\log\log n)$-bit certificates
- $\neg$Sym $\in$ dAMAM($\log n$)
- Other results on graph non-isomorphism

# Parameters

- Number of interactions between  and 
- Size of 

- Size of 
- Number of random 
- Shared vs distributed 

# Tradeoffs

[CFP, 2019]

- **Theorem 1** For every $c$, there exists a Merlin-Arthur (dMA) protocol for *triangle-freeness*, using $O(\log n)$ bits of shared randomness, with $\tilde{O}(n/c)$-bit certificates and $\tilde{O}(c)$-bit messages between nodes.

- **Theorem 2** There exists a graph property admitting a proof-labeling scheme with certificates and messages on $O(n)$ bits, that cannot be solved by an Arthur-Merlin (dAM) protocol with certificates on $o(n)$ bits, for any fixed number $k \geq 0$ of interactions between Arthur and Merlin, even using shared randomness, and even with messages of unbounded size.

# Proof of Theorem 1

Every node solves set-disjointness with each of its neighbors

We use a protocol by Aaronson-Wigderson (2009), recently revisited by Abboud, Rubinstein & Williams (2017)

Assume IDs in $\{1,\ldots,n\} = \{1,\ldots,n/c\} \times \{1,\ldots,c\} = [n/c] \times [c]$

Let $q = \Theta(nc)$ prime.

Node $u$ represents $N(u)$ as $c$ functions $F_{u,t} : [n/c] \to \{0,1\}$ s.t.

$$F_{u,t}(i) = 1 \Leftrightarrow (i,t) \in N(u)$$

Interpolation by $c$ polynomials $P_{u,t} : \mathbb{F}_q \to \mathbb{F}_q$ of degree $n/c-1$.

$N(u) \cap N(v) = \varnothing \Leftrightarrow P_{u,t}(i)\, P_{v,t}(i) = 0$ for every $i \in [n/c]$ and $t \in [c]$

Let $P_{u,v,t} = P_{u,t}\, P_{v,t}$ for every $v \in N(u)$ and $t \in [c]$

Let $P_u = \Sigma_{t\in[c]}\, \Sigma_{v\in N(u)}\, P_{u,v,t}$ of degree $\leq 2(n/c-1)$

Rmk: $u$ is not part of a triangle $\Leftrightarrow$ $P_u(i) = 0$ for every $i\in[n/c]$

Merlin assigns $Q_u$ to node $u$ using $O(n/c \log q)$ bits.

Arthur at node $u$ checks that:

(1) $Q_u(i) = 0$ for every $i\in[n/c]$

(2) $Q_u = P_u$

For (2), node $u$ picks $i^*$ u.a.r. in $\mathbb{F}_q$ and sends $\{ P_{u,t}(i^*), t\in[c] \}$ to all its neighbors, consuming bandwidth $O(c \log q)$ bits.

Node $u$ then computes $P_u(i^*) = \Sigma_{t\in[c]}\, \Sigma_{v\in N(u)}\, P_{u,t}(i^*)\ P_{v,t}(i^*)$

Node $u$ accepts if $Q_u(i^*) = P_u(i^*)$, and rejects otherwise.

The probability that two non-equal polynomials on $\mathbb{F}_q$ of degree at most $2(n/c-1)$ are equal at a random point $i^*$ is at most $2(n/c-1)/q < 1/3$ as $q = \Theta(nc)$. ❒

# Diameter (unweighted graphs)

- diam 2 vs. 3 requires $\Omega(n)$ rounds in CONGEST
- diam 3 vs. 4 requires certificates on $\Omega(n)$ bits for $\Sigma_1$LD
- $\tilde{O}(n)$ bits suffices for $\Sigma_1$LD, even for weighted graphs
- diam 5 vs. 6 requires certificates on $\Omega(n)$ bits for dMA [FMORT, 2019]

# Open problem for QuData