


# Local Verification of Global Proofs

Laurent Feuilloley<sup>1</sup>

University Paris Diderot, France

feuilloley@irif.fr

 <https://orcid.org/0000-0002-3994-0898>

Juho Hirvonen<sup>2</sup>

University of Freiburg, Germany

juho.hirvonen@cs.uni-freiburg.de

---

## Abstract

In this work we study the cost of local and global proofs on distributed verification. In this setting the nodes of a distributed system are provided with a nondeterministic proof for the correctness of the state of the system, and the nodes need to verify this proof by looking at only their local neighborhood in the system.

Previous works have studied the model where each node is given its own, possibly unique, part of the proof as input. The cost of a proof is the maximum size of an individual label. We compare this model to a model where each node has access to the same global proof, and the cost is the size of this global proof.

It is easy to see that a global proof can always include all of the local proofs, and every local proof can be a copy of the global proof. We show that there exists properties that exhibit these relative proof sizes, and also properties that are somewhere in between. In addition, we introduce a new lower bound technique and use it to prove a tight lower bound on the complexity of reversing distributed decision and establish a link between communication complexity and distributed proof complexity.

**2012 ACM Subject Classification** Theory of computation → Distributed computing models, Theory of computation → Proof complexity

**Keywords and phrases** Proof-labeling schemes, distributed verification, non-determinism, local proofs

**Digital Object Identifier** 10.4230/LIPIcs.DISC.2018.25

**Acknowledgements** The authors would like to thank Jukka Suomela for mentioning that AMOS could be an interesting problem in this context, and the anonymous reviewers for their feedback.

## 1 Introduction

In distributed decision a distributed system must decide if its own state satisfies a given property. When compared to classical decision problems, the crucial difference is that each node of the distributed system must make its own local decision based only on information available in its local neighborhood. We say that the system *accepts* if all nodes accept, and otherwise the system *rejects*.

A distributed system is modeled as a communication graph where edges denote nodes that can directly communicate with each other. The setting where each node only gets to see its constant-radius neighborhood in the graph is called *local decision* [8]. It is possible to

---

<sup>1</sup> Additional support from ANR project DESCARTES and INRIA project GANG.

<sup>2</sup> Supported by Ulla Tuominen Foundation.



decide local properties of the system in this manner, for example whether a given coloring is correct. On the other hand, it is impossible to decide global properties like whether a given set of edges forms a spanning tree.

To decide global properties, nodes can be provided with a nondeterministic proof, called a *proof-labeling scheme* [14] or a *locally checkable proof* [11]. Each node gets its own proof string as an additional input. Nodes can gather all the information in their constant-radius neighborhood, including these local proof strings, and decide to accept or reject. We say that such a scheme decides a property if there exists an assignment of local proofs to make all nodes accept if and only if the system satisfies the required property.

For example, to prove that a given set of edges forms a spanning tree, each node can be provided with the name of a designated root of the tree, and its distance to the root. Nodes can check that they agree on the identity of the root, and that they have exactly one neighbor with smaller distance to the root along the edges of the spanning tree.

We are interested in minimizing the size of the proof. In particular, we want to minimize the size of the largest label given to a single node. The local proofs often contain redundant information between the different local proof strings. For example, in the previous case each node must know the name of the root. The distances to the root are also highly correlated between neighbors. We approach this question by comparing the size of local proofs to *global* proofs. In this setting each node has access to the same universal proof string. The decision mechanism remains otherwise the same.

It is easy to see that minimum sizes of global and local proofs bound each other. A global proof can simply be a list of the local proof strings. Conversely, a local proof can copy the same global proof for each node. In this work, we study how these two proof sizes relate to each other for different properties.

Unlike in the centralized setting, distributed decision cannot be reversed trivially. This is due to the fact that the distributed decision mechanism is asymmetric: all nodes must accept a correct input, but a failure might only be detectable locally. Decision can be reversed using a logarithmic number of additional nondeterminism [11, 7]: when deciding a language  $\bar{L}$ , a spanning tree rooted at a rejecting node for  $L$  is constructed to convince the remaining nodes that such a node exists. This is an even more general primitive in distributed proofs: the proof must convince the nodes that a local defect exists somewhere in the graph, and only the nodes that are located close to this defect can verify its existence. We show that the existing upper bounds are asymptotically tight: reversing decision requires a local proof of logarithmic size, and global proofs do not help.

Since the distributed verification of a proof happens locally, a distributed proof of a global property must carry information between distant parts of the input graph. This has led to the use of lower bound techniques from communication complexity for distributed decision. On the other hand proving lower bounds inside the nondeterministic hierarchy of local decision [7] with multiple levels of nondeterminism seems to be hard. This is partially due to the fact that current lower bound techniques from communication complexity cease to work. We formalize this intuition by establishing a connection between the nondeterministic local decision hierarchy and the nondeterministic communication complexity hierarchy [1]. This connection exists for local proofs but is even stronger when considering global proofs.

**Motivation.** The first proof-labeling schemes were designed in the context of self-stabilizing algorithms, where a distributed algorithm would, in addition to the output, keep some information to verify that the state of the network is not corrupted. Similar scenarios exist for global proofs. For example, one may consider a network where the machines compute in

a distributed fashion, but an external operator with a view of the whole network can once in a while broadcast a piece of information, such as the name of a leader. As one expects this type of update to be costly, the focus is on minimizing the size of such broadcast information.

Our research belongs to a recent line of work that establishes the foundations of a theory of complexity for distributed network computation. In this context, the certificate comes from a prover, and one studies the impact of non-determinism on computation and the minimal amount of information needed from the prover to decide a task. Global proofs are a natural alternative form of non-determinism. Moreover, in proof-labeling schemes a part of the certificate is often global. For example, the name of a leader is given to all nodes. Global proofs can be used to study how much of such redundant information a local proof must have. Finally, one may consider that global proofs are the most natural equivalent of classical non-determinism: only the algorithm is distributed and we ask what is the cost if distributing the proof.

**Related work.** Proof-labeling schemes have been defined in [14, 15]. An important result in the area is the tight bound on the size of the proofs certifying minimum spanning tree [13]. Recently, several variations have been defined, for verifying approximation [3], with non-constant verification radius [20], with a dependency between the number of errors and the distance to the language [6], and variations on the communication model [22]. An analogue of the polynomial hierarchy for distributed decision has been defined [7].

Another line of work uses a slightly different notion of non-determinism. Fraigniaud et al. [8] consider a similar kind of scheme with a prover and local verifier, but with the constraint that the certificates should not depend on the identifiers of the network. For these works, and more generally the complexity theory of distributed decision, we refer to a recent survey [5].

The idea of a prover for computation in a network, or in a system with several computational units, appears outside of distributed computing, and usually with a global proof. In property testing, models where a prover provides a certificate to the machine that queries the graph have been considered [19, 12]. In two-party communication complexity, non-determinism comes as a global proof that both players can access. Along with non-determinism the authors of [1] define a hierarchy. Separating the levels of this hierarchy is still a major open problem [10].

**Our contributions.** We formalize the notion of *global proofs* for nondeterministic local verification. We study them, in particular comparing the global and local proof complexities of distributed verification.

One main goal of this line of research is to understand the price of locality in nondeterministic distributed verification – that is, how much information must be repeated in the local proofs of the nodes in order to allow local decision of global problems.

1. We show that the price of locality can exhibit the extreme possible values. An example of a maximally *global* property for distributed verification is the language where at most one node is selected. This is one of the core primitives in distributed verification: proving that at most one event of a given type happens in the whole graph. On the other hand, we show that when verifying that at least one node is selected, a global proof must use enough bits to essentially copy every local proof label.
2. We introduce a new proof technique for proving lower bounds for local verification. This proof technique is based on analyzing the neighborhood graph labeled with the local proofs. We use it to show that reversing decision requires  $\Omega(\log n)$ -bit local proof and a  $\Omega(n \log n)$ -bit global proof. Our proof technique is somewhat similar to the one used by

Göös and Suomela to prove their  $\Omega(\log n)$  lower bounds for local proofs [11]. Their proof technique relies on combining several fragments of *yes*-instances to produce an accepting *no*-instance. This is not sufficient for our results, since we want to prove lower bounds for languages for which several fragments of *yes*-instances joined together might still produce a *yes*-instance.

3. We establish a connection between nondeterministic verification and nondeterministic communication complexity. Proving separations for the hierarchy of nondeterministic communication complexity has been an open question since its introduction over 30 years ago [1]. We show that proving similar separations for the hierarchy of nondeterministic local decision is connected to this question: for every boolean function  $f$  we construct a distributed language such that it can be decided on the  $k$ th level if  $f$  can be decided on the  $k$ th level of the communication complexity hierarchy. Considering global proofs instead of local proofs allows to strengthen this result as in this new setting one can also show that verification schemes imply communication protocols. This formalizes the previous intuition that proving lower bounds for nondeterministic local verification is potentially hard as it would imply proving lower bounds for nondeterministic communication complexity.

## 2 Model and definitions

The network is modeled by a simple graph  $G = (V, E)$ . The size of the graph  $|V|$  is denoted by  $n$ . The nodes are given unique identifiers from a range that is polynomial in  $n$  and therefore can be encoded with  $O(\log n)$  bits.

**Distributed decision.** A *distributed language* is a set of labeled graphs  $(G, x)$ , where  $x$  is a function that assigns input labels to nodes and edges of  $G$ . Distributed languages are often assumed to be computable (from the centralized computing perspective), but this is irrelevant for the current paper. An example is the language SPANNING TREE, which is the set of graphs whose edges are labeled with 1 or 0 such that edges labeled with 1 form a spanning tree of the graph.

A *distributed proof*  $\ell: V(G) \rightarrow \{0, 1\}^k$  is a function that assigns a string of bits (also called a *certificate*) to each node of the graph. Each node gets its own string as a part of its input. The *size* of a proof is the length of the proof strings  $k$ .

A *local decision algorithm* (also called a *verifier*) with radius  $t$  is a distributed algorithm  $A$ , in the synchronous message passing model, in which every node  $v$  first gathers all the information about its  $t$ -radius neighborhood (the structure of the graph, the identifiers of the nodes, the local inputs), and possibly some proofs given by one or several provers, and outputs a decision, *accept* or *reject*, based on this information. The distance  $t$  is constant independent of  $n$ , the size of the network, and therefore the algorithm can be seen as a function  $A(v, x, \ell)$  on the local graph topology, the inputs labels, and the possible proof. The verifier is assumed to be uniform, that is, it does not know the size of the graph.

A *local decision scheme* is simply a local decision algorithm, and we say that it decides a language  $L$  if, for every labeled graph, all nodes accept if and only if the labeled graph belongs to  $L$ :

$$\forall(G, x) : (G, x) \in L \iff \forall v \in V(G), A(v, x) = \text{accept}.$$

A *nondeterministic decision scheme* consists of a local decision algorithm and a *prover* that assigns a distributed proof to each node. A nondeterministic scheme exists for a language  $L$

if there is an algorithm  $A$  such that for every labelled graph  $(G, x)$  there exists a proof that makes every node accept if and only if  $(G, x)$  belongs to the language:

$$\forall(G, x) : (G, x) \in L \iff \exists \ell \forall v \in V(G), A(v, x, s) = \text{accept}.$$

In particular, if  $(G, x) \notin L$ , then there must not exist a proof that makes all nodes of  $G$  accept.

**Different types of proofs.** We study three different variants of distributed proofs. In a (*purely*) *local proof*, the prover provides every node with its own label. The local proofs have the same size which depends only on the language and on the size of the network  $n$ . For a given language, the minimum, over all proofs, of the maximum proof size at a single node is denoted by  $s_\ell(n)$ . This is the classic framework of proof-labeling schemes. We introduce (*purely*) *global proofs*, where the prover provides a single certificate, and every node can access it. This can also be seen as a local proof that must assign the same string to every node. Its minimum size is denoted by  $s_g(n)$ . Finally, in *mixed proofs*, the prover provides a global proof and local proofs. The size considered, denoted by  $s_m(n)$ , is the sum of the size of the global proof, and the size of the concatenation of the local proofs in an optimal scheme.

### 3 The price of locality

In this section, we study the size of local, mixed and global proofs for different problems, and the price of locality that follows.

#### 3.1 Proof sizes

In this subsection some general inequalities between the sizes of the different proof sizes are proven. We then discuss the definition of the price of locality.

► **Theorem 1.** *For any language, the optimal proof sizes respect the following inequalities.*

$$s_\ell(n) \leq s_m(n) \leq s_g(n) \tag{1}$$

$$s_m(n) \leq n \cdot s_\ell(n) \tag{2}$$

$$s_g(n) \leq n \cdot s_\ell(n) + O(n \log n). \tag{3}$$

**Proof.** The first line of inequalities mainly follows from the definitions. Suppose one is given a mixed certificate for a language, with local certificates of size  $f(n)$  each, and a global certificate of size  $g(n)$ . The size of this mixed certificate is  $s_m(n) = n \cdot f(n) + g(n)$ . Then one can create a local proof of size  $f(n) + g(n)$ , by giving to every node its local part concatenated with the global part. Thus  $s_\ell(n) \leq s_m(n)$ . The inequality  $s_m(n) \leq s_g(n)$  holds because the mixed proof is a generalization of the global proof. Similarly, if there exists local certificates of size  $s_\ell(n)$ , then one can use them in the mixed model. The size measured in the mixed model will then be  $n \cdot s_\ell(n)$ . Finally, given local certificates, one can craft a global certificate. The global certificate consists of a list of pairs, each pair consisting of an ID and the local certificate of the node with this ID. The size is in  $n \cdot s_\ell(n) + O(n \log n)$  because identifiers are on  $O(\log n)$  bits. ◀

### 3.2 Price of locality

We define the *Price of Locality* for distributed proofs, by analogy with the *Price of Anarchy* in algorithmic game theory [16, 21]. Note that this is not the same as the price of locality that appears in the title of [17]. The price of locality (PoL) of a language is defined as the ratio between the size of the concatenation of the purely local certificates, divided by the size of the mixed certificate. That is:

$$PoL(n) = \frac{n \cdot s_\ell(n)}{s_m(n)}.$$

It may come as a surprise that we use mixed proofs instead of global proofs for this definition. There are several reasons for this. First, the inequalities above insure that with this definition the ratio is between 1 and  $n$ , whereas with global proofs the price could be smaller than 1, thus not a price per se. We study this possibility in Section 5. More fundamentally, mixed proofs are a better way to measure how much it costs to fully distribute a proof, as they are a proper generalization of the local proofs, which is not the case of global proofs. Second, our upper bounds use purely global proofs, and our lower bounds (except in Section 5) consider mixed proofs, thus we get the strongest results on both sides.

► **Remark.** Note that we assume that the local proofs given to the nodes are of the same size, and thus the concatenation is exactly  $n$  times larger than the size of one local certificate. The interesting question of whether the average proof size could be asymptotically better, if proofs of different sizes were allowed, is outside of the scope of this paper.

### 3.3 High price of locality

In this section, we prove that it can be very costly to distribute the proof. This is easy and is a warm-up for the rest of the paper. A scheme uses *uniform local proofs*, if the local proofs given to the nodes of the network are all equal. It is simple to change such proof system into a global proof: just take the uniform local proof and make it global. The verifier has the same behaviour and the scheme is correct. This implies the following theorem.

► **Theorem 2.** *For languages where an optimal proof-labeling scheme uses uniform local proofs, the price of locality is  $\Theta(n)$ .*

This theorem applies to the language SYMMETRY, the set of graphs that do not admit a non-trivial automorphism, which has an optimal scheme with  $O(n^2)$  uniform local proofs [11]. We now consider the language AT-MOST-ONE-SELECTED (AMOS), that has been defined and used in [9]. In this problem, the nodes are given binary inputs, and the *yes*-instances are the ones such that at most one node has input 1. We prove that this language meets the hypothesis of the previous theorem.

► **Theorem 3.** *The language AMOS has an optimal proof-labeling scheme with uniform proofs of size  $O(\log n)$ .*

**Proof.** We describe the scheme. The prover's strategy on *yes*-instances is the following. If there is exactly one selected node, the prover provides the ID of the node as uniform certificate, otherwise it provides an empty label. The verification algorithm is, for every node  $v$ : if  $v$  is selected and the certificate is not its ID, then reject, otherwise accept. It is easy to check that this scheme is correct. First, if no node is selected, all nodes accept, for all certificate. Second, if one nodes is selected, then the prover provides its ID as a certificate, and thus the selected node accepts, and all the other nodes too. Finally, if two or more nodes are selected, at most one of them has its ID written in the global certificate, because the IDs are distinct and thus at least one node is rejecting. ◀

In [11], the authors prove that the language LEADER ELECTION, where exactly one node is labelled 1 and the remaining nodes are labelled 0, requires  $\Omega(\log n)$  local certificate. The proof basically shows that without this amount of proof, an instance with two leaders would be accepted. This reasoning holds for AMOS, and we can derive a  $\Omega(\log n)$  lower bound for local certificates as well.

► **Corollary 4.** *The price of locality for AMOS is in  $\Theta(n)$ .*

### 3.4 Intermediate price of locality

In this subsection, we show that the language MINIMUM SPANNING TREE (MST) has price of locality  $\Theta(\log n)$ . It is an intermediate price, between  $n$  (the previous subsection), and constant (the next section). The language MST is the set of weighted graphs in which the subset of the edges labelled with 1 form a minimum spanning tree of the graph. The edge weights are assumed to be polynomial in  $n$  and for simplicity we assume that the edge weights are distinct.

In [13], the authors show that there exist local proofs of size  $O(\log^2 n)$  for MST, and that this bound is tight. We show a simple global proof that has size  $O(n \log n)$ . As a mixed proof for the simpler language SPANNING TREE requires  $\Omega(n \log n)$  (see Section 4), this bound is also tight.

► **Theorem 5.** *The global proof size for MINIMUM SPANNING TREE is in  $O(n \log n)$ .*

**Proof.** We describe the scheme. On a *yes*-instance the prover provides a list of the selected edges with their weights. This global certificate has size  $O(n \log n)$ , because the edge weights and the identifiers can be written on  $O(\log n)$  bits. Then every node first checks that the certificate is correct regardless of the graph. That is, every node checks that:

- The certificate is a well-formed edge list. Let  $L$  be this list.
- The list  $L$  describes an acyclic graph. That is that there is no set of nodes  $w_1, w_2, \dots, w_k$  such that  $(w_1, w_2), (w_2, w_3), \dots, (w_{k-1}, w_k)$ , and  $(w_k, w_1)$  appear in the list.
- The list  $L$  describes a connected graph. That is for any pair of nodes present in the list, there exists a path in the list that connects them.

Then every node  $v$  of the graph checks locally that:

- The  $L$  is consistent with the selected edges that are adjacent to it.
- It has an adjacent selected edge.
- For every  $e = (v, w)$  in the graph but not in the list, and every edge  $e'$  on the path from  $v$  to  $w$  in  $L$ , the weight of  $e'$  is smaller than the weight of  $e$ .

We now prove the correctness of the scheme. The first part of the verification insures that the set of edges described by  $L$  form an acyclic connected graph. The two first checks of the second part insure that it contains the selected edges and that it is spanning the graph. As it is a spanning tree, it must then be exactly the set of selected edges. Finally, remember that the so-called *cycle property* states that a spanning tree verifying the last item of the previous algorithm is a minimum spanning tree [4]. ◀

## 4 Locality for free and reversing decision

In this section, we show that for some languages there exists local proofs of size  $O(\log n)$  and that any mixed proof has size  $O(n \log n)$ . It follows that in this case, the price of locality is constant, that is the locality of the proofs comes for free.

The language we consider, called AT LEAST ONE SELECTED (ALOS), consists of all labeled graphs such that at least one node has a non-zero input label. We say that a node with a non-zero input label is *selected*. Proving that at least one node has some special property (being the root, having some input, being part of some special subgraph) is an important subroutine in many schemes.

On a more fundamental perspective, reversing decision basically deals with proving that some node is rejecting, which falls into the scope of the ALOS. It has long been known that  $O(\log n)$  local proof is sufficient for reversing decision, and the current section shows that not only is this optimal, but also one cannot gain by using global proofs.

► **Theorem 6.** *A mixed proof for the language ALOS requires  $\Omega(n \log n)$  bits.*

The theorem is equivalent to stating that the language requires either  $\Omega(\log n)$  bits per local proof or an  $\Omega(n \log n)$  bit global proof.

**Proof of Theorem 6.** The proof is essentially a counting argument that shows that for any proof scheme that uses small certificates we can find a graph in which no nodes are selected, but there is a proof that makes the verifier accept the input. This is done by analyzing the structure of the graph where nodes are all possible accepting labelled cycle fragments, and two nodes are adjacent if the verifier accepts locally when they are placed one after the other on a cycle. Finally we show that this graph contains an accepting cycle that has no selected nodes.

Consider a mixed scheme with local certificates of size  $f(n)$  and a global certificate of size  $g(n)$ . Let  $r$  be the verification radius of the scheme.

**Blocks.** The lower bound instances are consistently oriented cycles of length at most  $n = (b + 1)(2r + 1)$ , for some integer  $b$ . Cycles are constructed from blocks of  $2r + 1$  nodes: the  $i$ th block is a path  $B_i = (v_j, v_{j+1}, \dots, v_{j+2r})$ , where  $j = i(2r + 1) + 1$ , oriented consistently from  $v_j$  to  $v_{j+2r}$ . Each node  $v_j$  is labeled with the unique identifier  $j$ .

**Constructing instances from blocks.** Let  $\pi: [b] \rightarrow [b]$  be a permutation on the set of the first  $b$  blocks. Each permutation defines a cycle  $C_\pi$  where we take the blocks in the order given by  $\pi$ , and finally take the  $(b + 1)$ th block. Each pair of consecutive blocks in  $\pi$  is connected by an edge, and  $B_{b+1}$  is connected to  $B_{\pi^{-1}(1)}$ .

Finally, the center node  $v_{b(2r+1)+r+1}$  of  $B_{b+1}$  is labeled with a non-zero label, making the instance a *yes*-instance. All other nodes are labeled with the zero-label. Denote this family of permuted *yes*-instances by  $\mathcal{C} = \{C_\pi\}_\pi$ .

**Labeled blocks.** The prover assigns a local proof of  $f(n)$  bits to each node. Thus, there are  $2^{f(n)(2r+1)}$  different possible labeled versions of each block. We call these *labeled blocks*. Denote by  $B_{i,\ell}$  the block  $B_i$  labeled according to  $\ell$ . We call  $B_i$  the *type* of  $B_{i,\ell}$ .

Consider two labeled blocks,  $B_{i,\ell}$  and  $B_{j,\ell'}$ , in this order, linked by an edge. We say that labeled blocks are accepting from  $B_{i,\ell}$  to  $B_{j,\ell'}$  with global certificate  $L$  if, when we run the verifier on the nodes that are at distance at most  $r$  from an endpoint of the connecting edge, all these nodes accept. We denote this by  $B_{i,\ell} \rightarrow_L B_{j,\ell'}$ .

For each choice  $L$  of the global certificate, this edge relation defines a graph  $G_{\mathcal{B},L}$  on the set of labeled blocks. A path in  $G_{\mathcal{B},L}$  corresponds to a labeled path fragment in which all nodes at least  $r$  steps away from the path's endpoints accept. Finally, an accepting cycle is a cycle in  $G_{\mathcal{B},L}$  such that all nodes accept.



**Bounding the overlap of certificates.** For each  $C_\pi \in \mathcal{C}$ , there must exist an accepting assignment of certificates to the nodes. Let  $L$  denote the global part of this accepting certificate. Such a  $C_\pi$  corresponds to a directed cycle in  $G_{\mathcal{B},L}$ . Note that in this cycle the last edge can be omitted as it would always link the last block to the first block. Then  $C_\pi$  corresponds to a directed path  $P(C_\pi, L)$  of length  $b$  in  $G_{\mathcal{B},L}$ . Denote the set of labeled blocks on this path by  $S(C_\pi, L)$ .

Let  $\mathcal{C}_L$  denote the set of instances such that there exists an accepting local certification given the global certificate  $L$ . Every *yes*-instance has an accepting certification, so there must exist  $L^*$  with

$$|\mathcal{C}_{L^*}| \geq |\mathcal{C}|/2^{g(n)}.$$

Now consider any two instances  $C_\pi$  and  $C_{\pi'}$  in  $\mathcal{C}_{L^*}$ . We drop the specification of the global certificate from the notation. We have the following lemma.

► **Lemma 7.** *For all pairs of instances  $C_\pi, C_{\pi'}$  with the same accepting global certificate  $L$ , we have that  $S(C_\pi, L) \neq S(C_{\pi'}, L)$ .*

**Proof.** Assume that  $C_\pi$  and  $C_{\pi'}$  use the same set of blocks, that is  $S(C_\pi, L^*) = S(C_{\pi'}, L^*)$ . Also assume without loss of generality, that  $\pi$  is the identity permutation. Now in  $P(C_{\pi'})$  there must exist a *back edge* with respect to  $\pi$ , that is, an edge between labeled blocks  $B$  and  $B'$ , of types  $B_{\pi'^{-1}(i)}$  and  $B_{\pi'^{-1}(i+1)}$  respectively, such that  $\pi'^{-1}(i) > \pi'^{-1}(i+1)$ . This is because we assumed that the instances consist of the same blocks, but are different. Therefore at some point an edge of  $C_{\pi'}$  must go backwards in the order of  $\pi$ . We also have that  $B, B' \neq B_{b+1}$  as if there is no back edge before reaching  $B_{b+1}$ , we must have  $C_\pi = C_{\pi'}$ .

This implies that there is an accepting cycle formed by taking first the path from  $B$  to  $B'$  along  $P(C_\pi)$  and then an edge from  $B'$  to  $B$ . This cycle does not contain a selected node. It follows that there is a *no*-instance of size at least  $2(2r+1)$  and a certification that causes the verifier to accept the instance, a contradiction. ◀

► **Remark.** Note that the contradicting instances can be of size  $2(2r+1)$  but the identifiers can be of size  $n$  and the certificates of size  $f(n)$ . Therefore the lower bound only holds for uniform verifiers that do not get any guarantees except that 1) the identifiers come from the set  $[n+c]$ , for some constant  $c$ , and 2) the certificates are of size at least  $f(n)$ .

Alternatively it is possible to consider ALOS on possibly disconnected instances so that every connected component must have at least one node selected. In this case the proof will fool even a non-uniform scheme (that is, one that has information about the real size of the instance).

**Counting argument.** By Lemma 7, each pair of permutations  $\pi, \pi'$  in  $\mathcal{C}_{L^*}$  must induce a different set of labeled blocks that form the accepting certifications of instances  $C_\pi$  and  $C_{\pi'}$ . The number of different permutations in  $\mathcal{C}_{L^*}$  is at least  $b!/2^{g(n)}$ . On the other hand, the number of different sets of labeled blocks, selecting a block of each type, is  $2^{f(n)(2r+1)b}$ . As shown in Lemma 7, to have a legal certification, we must have that  $2^{f(n)(2r+1)b+g(n)} \geq b!$ .

Using Stirling's approximation we get that  $f(n)(2r+1)b + g(n) \geq b \log_2 b - (\log_2 e)b + O(\ln b)$ . Since  $b = \Theta(n)$  and  $r = O(1)$ , this implies that either  $f(n) = \Omega(\log n)$  or  $g(n) = \Omega(n \log n)$ . Thus the mixed proof has size  $\Omega(n \log n)$ . ◀

Theorem 6 implies that reversing decision requires  $\Omega(\log n)$  bit certificates in the following sense.

► **Corollary 8.** *There exists a language, NONE SELECTED, that can be decided locally without nondeterministic proofs and its complement is ALOS, which requires local certificates of size  $\Omega(\log n)$  or global certificates of size  $\Omega(n \log n)$ .*

**Proof.** Consider the language NONE SELECTED, that is, the language of labeled graphs such that all nodes have the zero label. This language is locally decidable without nondeterminism, that is, NONE SELECTED  $\in$  LD [8] or  $\Lambda_0$  in the notation of Section 6. The language ALOS is its complement. Finally, by Theorem 6, deciding ALOS, that is, reversing the decision of NONE SELECTED requires local certificates with  $\Omega(\log n)$  bits or global certificates with  $\Omega(n \log n)$  bits. ◀

The proof can be adapted to several other problems, namely leader election, spanning tree and the set of odd cycles, giving a lower bound for mixed proof systems.

► **Corollary 9.** *Any mixed proof system for LEADER ELECTION requires local certificates of size  $\Omega(\log n)$  or global certificates of size  $\Omega(n \log n)$ .*

**Proof of Corollary 9.** Consider the proof of Theorem 6. The family  $\mathcal{C}$  of *yes*-instances for ALOS is also a family of *yes*-instances for LEADER ELECTION. Since LEADER ELECTION  $\subsetneq$  ALOS, the proof of Theorem 6 produces *no*-instances of LEADER ELECTION that the verifier accepts. ◀

► **Corollary 10.** *Any mixed proof system for SPANNING TREE requires local certificates of size  $\Omega(\log n)$  or global certificates of size  $\Omega(n \log n)$ .*

**Proof sketch.** Consider two types of instances: the cycles where all the edges are selected, and the the cycles where all edges but one are selected. The first instances are not in the language, the second are. We can rephrase this restricted problem as: there is at least one non-selected edge. Then the same type of proof works. ◀

► **Corollary 11.** *Any mixed proof system for ODD-CYCLE requires local certificates of size  $\Omega(\log n)$  or global certificates of size  $\Omega(n \log n)$ .*

**Proof sketch.** The proof of Corollary 11 consists in a refinement of the proof for ALOS. We can build on an odd number of blocks, each block being of odd length itself. Then we can give a colour to each block so that half of the blocks are black and half are white. Finally we can force the paths to alternate between white and black blocks. The cycles obtained will then be of even length, and thus be *no*-instances. The number of possible paths is reduced, but only by term of the form  $2^b$ , which is negligible compared with the  $b!$  term. The calculation then still gives the  $\Omega(n \log n)$  lower bound. ◀

A consequence of these corollaries is that all the  $\Omega(\log n)$  lower bounds obtained in [11] for local certificates can be lifted to  $\Omega(n \log n)$  mixed proofs with our technique. However for the problem AMOS we studied in the previous section, our technique does not work, which is consistent with the fact that an  $\Omega(n \log n)$  lower bound would contradict the  $O(\log n)$  upper bound we show. As already said, the technique of [11] works for AMOS, and provides the  $\Omega(\log n)$  bound for local proofs. The reason our technique fails is because we show that if the certificates are too short then one can shorten the cycles that are *yes*-instances, which is not useful for AMOS, as a ‘subinstance’ of this problem is still in the language: one can only remove selected nodes. The authors of [11] show that one can glue different *yes*-instances together and get a configuration that is still accepted by the nodes, and for AMOS this means one can glue different instances with one node selected, and then get an instance with more

than one node selected, and this instance is still accepted, which raises a contradiction. Note that because of this duality, the proof technique of [11] does not give a lower bound for ALOS, even for the case of local proofs.

It is also worth noting that the intersection of the languages AMOS and ALOS is LEADER ELECTION. It is known that LEADER ELECTION has a proof-labeling scheme of size  $\Theta(\log n)$ , constructed with a spanning tree, along with the ID of the leader given to all the nodes. The results of the current and previous sections show that this decomposition is mandatory: one needs a global part of size  $\Theta(\log n)$ , and a local part of size  $\Theta(\log n)$ .

## 5 Beyond free locality

The language BIPARTITE is the set of bipartite graphs. Local proofs of constant size exist for this language: the prover can just describe a 2-coloring of the graph by giving a bit to each node, and every node can check that its neighbors are given a color different from its own. We conjecture that for this language, even when restricting the topology to cycles, optimal purely global proofs are larger than the sum of the optimal local proof sizes. More precisely this sum is  $\Theta(n)$ , and we conjecture that purely global proofs take  $\Theta(n \log n)$  bits.

► **Conjecture 12.** For BIPARTITE, purely global proofs have size  $\Theta(n \log n)$ .

We are not able to prove the lower bound of the conjecture, but we can prove weaker inequalities. For this problem, the range of the identifiers is important, and that is why we consider the maximum identifier to be a parameter  $M$ , that we do not bound by a polynomial any more.

► **Theorem 13.** For BIPARTITE, there exist two constants  $\alpha$  and  $\beta$  such that, for identifiers bounded by  $M$ :

$$\alpha \max\{n, \log \log M\} \leq s_g(n) \leq \beta \min\{M, n \log M\}.$$

Note that if  $M = n$  then we get a tight  $\Theta(n)$  bound. The  $\Omega(n)$  lower bound holds for any ID range, but the  $\log \log M$  bound shows that this cannot be tight for every ID range: we can get an arbitrarily large lower bound if we allow arbitrarily large identifiers.

**Proof.** We start with the upper bounds. The  $O(n \log M)$  upper bound comes from the certificate made by concatenating the couples (ID, local proof) for every node, as in Theorem 1. For the  $O(M)$  upper bound, the prover strategy is to provide a vector with  $M$  cells, where cell  $i$  will contain a bit indicating the color of the node with ID  $i$ . In both cases the nodes will get their own colors and the colors of their neighbors from the certificate, and they can check locally the consistency of the coloring.

We now prove the lower bounds for the restricted case of cycles. Note that bipartiteness on cycles boils down to distinguishing between odd and even length cycles. A priori, in a scheme for this language, the prover is not forced to explicitly provide a coloring to the nodes. We show that a proof always implies a coloring. More precisely, a node can always extract from the proof its color and the colors of its neighbors, and then check the consistency of the coloring. As in Section 4, we will use blocks of nodes to build a large a number of instances. The blocks are paths of  $2r + 1$  nodes. The  $i$ -th block, noted  $b_i$  has consecutive IDs from  $i(2r + 1) + 1$  up to  $(i + 1)(2r + 1)$ . Every block is oriented in the direction of increasing IDs. A *block-based cycle* is a cycle made by concatenating blocks, with a consistent orientation.

► **Lemma 14.** *For every global proof  $c$ , there exists a coloring function  $f_c : [M] \mapsto \{0, 1\}$ , such that for every block-based cycle  $H$  that is accepting with certificate  $c$ ,  $f_c$  defines a proper coloring of  $H$ .*

**Proof of Lemma 14.** First, note that as the blocks have odd length, a block-based cycle has even length if and only if it is composed of an even number of blocks. Then, for block-based cycles, replacing virtually each block by a vertex, and trying to 2-color the resulting cycle is equivalent to 2-color the nodes of the original instance.

Fix a certificate  $c$ . Consider the directed graph  $G_c$ , whose nodes are the blocks  $(b_i)_i$ . There is an oriented edge  $(b_i, b_j)$  if and only if there exists a block-based cycle for which  $c$  is an accepting certificate, and where the block  $b_i$  is followed by the block  $b_j$ .

► **Claim 15.** *The graph  $G_c$  contains no directed odd cycle.*

**Proof of Claim 15.** Suppose the graph  $G_c$  contains a directed odd cycle. Consider the corresponding block-based cycle  $C$ . Because it has odd length, it is a *no*-instance. Consider a node  $v$  of this instance that is rejecting with certificate  $c$ . Without loss of generality, assume it is in the first half of its block  $b_i$  (that is, its ID is between  $i(2r+1)+1$  and  $i(2r+1)+r+1$ ). Let  $b_h$  be the block preceding  $b_i$  in  $C$ . The node  $v$  can only see (parts of) of  $b_h$  and  $b_i$ , because its radius is  $r$ . As  $(b_h, b_i)$  belongs to  $G_c$ , there exists a *yes*-instance  $C'$ , in which every node accepts with proof  $c$ , and in which  $b_i$  follows  $b_h$ . This is a contradiction, because with certificate  $c$ ,  $v$  is accepting in  $C'$ , and rejecting in  $C$ , although it has the exact same view in both instances. Thus the graph  $G_c$  contains no directed odd cycle. ◀

► **Claim 16.** *Every connected component of the graph  $G_c$  is strongly connected.*

**Proof of Claim 16.** Consider the following way of building  $G_c$ : take an arbitrary ordering of the cycles that accept with  $c$ , and add them (i.e. add their edges) to  $G_c$ , one by one. We show the strong connectivity of the connected components by induction. The property holds for the empty graph. Suppose every connected component is strongly connected until some step, and that we add a new cycle. As a directed cycle is strongly connected, merging it with one or several strongly connected components, keeps the strong connectivity. ◀

It is known that a strongly connected digraph with no odd length directed cycles can be 2-colored (see e.g. Theorem 1.8.1 in [2]). Thus, from Claim 15 and Claim 16, we get that  $G_c$  has a 2-coloring. This 2-coloring induces a 2-coloring on all the block-based cycles accepting with  $c$ , thus it defines the function  $f_c$  of the lemma. ◀

Now fix a size  $n$ , for an even  $n$ , and consider the following table. The columns are indexed by the blocks, thus there are  $M/(2r+1)$  of them. The rows are indexed by all the possible certificates, that is all the strings on  $s_g(n)$  bits. The cell that corresponds to block  $b$  and certificate  $c$  contains the color given by  $f_c$  to the center node of  $b$ . We will now give two simple properties of this table that will imply the two lower bounds.

Let a *balanced binary vector* be a vector of bits with the same number of zeros and ones. Let the *complement* of a binary vector be the same binary vector where ones and zeros have been complemented.

► **Lemma 17.** *For every balanced binary vector  $p$  of length  $n$ , there exists a row of the table such that the vector made by the  $n$  first cells is equal to either  $p$  or its complement.*

**Proof of Lemma 17.** Consider a balanced binary vector  $p$ . Consider a cycle  $H$  made by concatenating the  $n$  first blocks, in an ordering such that coloring block  $i$  with the  $i^{\text{th}}$  bit of  $p$ , defines a proper coloring of the cycle. Note that, as  $p$  is balanced, such a cycle must exist. This cycle  $H$  has even length, thus it belongs to the language and there exists an accepting certificate  $c$ . The first  $n$  cells of the row of  $c$  must describe a proper coloring of  $H$ , and there are only two such colorings:  $p$  and its complement. ◀

For every balanced vector of length  $n$  there exists a row that it matches (or its complement matches) on the  $n$  first cells. A row can only correspond to one such vector (up to complement), and since there are at least  $2^{n/2}/2$  balanced binary vectors (first  $n/2$  bits can be chosen freely) the table must have at least  $2^{n/2}$  rows. This means that there are at least  $2^{n/2}$  different certificates, thus the certificate size is lower bounded by  $n$ , up to multiplicative constants.

► **Lemma 18.** *Two columns of the table cannot be equal.*

**Proof of Lemma 18.** Suppose columns  $i$  and  $j$  are equal. Consider an even-length block-based cycle  $C$ , where the block  $i$  is linked to the block  $j$ . Such a cycle always exists. For every certificate  $c$ , the same color is given to both blocks  $i$  and  $j$  in  $f_c$ , because the columns are equal. Thus no certificate provides a proper coloring of  $C$ , which is a contradiction because  $C$  belongs to the language. ◀

As there are  $M$  different columns, there is at least order of  $\log(M)$  certificates. Then the length of a certificate is in  $\Omega(\log \log(M))$ . This finishes the proof of Theorem 13. ◀

## 6 Local decision and communication complexity

In this section we present the nondeterministic hierarchies for local decision and communication complexity.

**Nondeterministic hierarchy of local decision.** Feuilloley et al. [7] introduced a nondeterministic *hierarchy of local decision*. It is the distributed computing analogue of the classical polynomial hierarchy. A prover and a disprover take turns, providing each node with proofs of size  $O(\log n)$ . Once the proof labels have been assigned, the nodes look at their constant-radius neighborhood, including the nondeterministic proofs, and decide whether they accept or not.

The classes  $\Sigma_k$  and  $\Pi_k$  correspond to the languages that can be decided using  $k$  levels of nondeterminism – in  $\Sigma_k$  the prover goes first, and in  $\Pi_k$  the disprover. Let  $\ell_1, \ell_2, \dots, \ell_k$  denote the  $k$  levels of nondeterministic labels provided to the nodes. A language  $L \in \Sigma_k$  if and only if there exists a verifier  $A$  such that

$$(G, x) \in L \iff \exists \ell_1, \forall \ell_2, \dots, \mathbb{Q} \ell_k, \forall v \in V(G), A \text{ accepts.}$$

Here  $\mathbb{Q}$  denotes the existential quantifier if  $k$  is odd and the universal quantifier otherwise. The classes  $\Pi_k$  are defined similarly, but with the disprover (i.e. universal quantifier) going first.

The classes that corresponds to the disprover talking last collapse to the previous level, and the only interesting levels are  $\Sigma_1, \Pi_2, \Sigma_3, \dots$ , which are denoted by  $(\Lambda_k)_{k \in \mathbb{N}}$ . The complements of these classes are denoted by  $\text{co-}\Lambda_i$  and we have that  $\text{co-}\Lambda_k \subseteq \Lambda_{k+1}$  [7], i.e., decision can always be reversed using an extra quantifier with  $O(\log n)$  bits. As shown in Theorem 6, in general,  $\Omega(\log n)$  bits are also required for reversing decision.

The main open question of Feuilleley et al. [7] was whether  $\Lambda_2$  and  $\Lambda_3$  were different or not. As in the polynomial hierarchy, the equality  $\Lambda_k = \Lambda_{k+1}$  of two levels would imply a collapse of the local hierarchy down to the  $k$ th level. We show that this question is related to long-standing open questions nondeterministic communication complexity [1].

**A hierarchy for global certificates.** Similar to the hierarchy of local certificates, we can define a hierarchy for the global certificates. Define  $\Sigma_k^G$ ,  $\Pi_k^G$ , and  $\Lambda_k^G$  as previously, except that the labels  $\ell_1, \ell_2, \dots, \ell_k$  are global certificates seen by all nodes.

**Communication complexity.** We will compare the hierarchies of nondeterministic local decision to the hierarchy of nondeterministic communication complexity defined by Babai et al. [1].

In the communication complexity setting we are given a boolean function  $f$  on  $2n$  bits. Two entities, Alice and Bob, are each given  $n$ -bit vectors  $x$  and  $y$ , and have to decide if  $f(x \cup y) = 1$ . They can communicate through a reliable channel and have unlimited computational resources. The measure of complexity is the number of bits Alice and Bob need to communicate in order to decide  $f$ . For more details, see for example the book [18].

In nondeterministic communication complexity Alice and Bob have access to nondeterministic advice (we will say that it is given by a *prover*). The cost of a protocol is the sum of the number of bits communicated by Alice and Bob and the number of advice bits given by the prover. This means that messages of Alice and Bob can equivalently be encoded in the advice.

Babai et al. defined a hierarchy of nondeterministic communication complexity [1]. In addition to Alice and Bob we have two players, whom we will call *prover* and *disprover* for consistency, giving nondeterministic advice to Alice and Bob. Prover and disprover will alternate  $k$  times and each time give an advice string of  $g(n)$  bits. Now we define the class  $\Sigma_k^{cc}(g(n))$  of boolean functions as the set of functions such that there exists an algorithm  $A$  for Alice, and an algorithm  $B$  for Bob such that if  $f \in \Sigma_k^{cc}(g(n))$ , then

$$\forall x, y, \exists \ell_1, \forall \ell_2, \dots, \mathcal{Q} \ell_k A(\ell_1, \ell_2, \dots, \ell_k, x) = B(\ell_1, \ell_2, \dots, \ell_k, y) = 1 \iff f(x, y) = 1.$$

Again  $\mathcal{Q}$  denotes the existential quantifier if  $k$  is odd and the universal quantifier otherwise. The classes  $\Pi_k^{cc}(g(n))$  are defined similarly, but with the disprover going first. We are particularly interested in this hierarchy when  $g(n) = O(\log n)$ . Note that in their work, Babai et al. consider the hierarchy for  $g(n) = O(\text{poly}(\log n))$  [1].

## 6.1 Connecting local decision and communication complexity

In this section we partially formalize the intuition that complexity of local verification is connected to communication complexity. We show that general lower bound proof techniques for nondeterministic local verification will also apply to communication complexity. We then show that if one considers global proofs instead of local ones, the result can be strengthened.

► **Theorem 19.** *For every boolean function  $f$ , there exists a distributed language  $L_f$  such that if  $f \in \Sigma_k^{cc}(g(n))$  for odd  $k$  or  $f \in \Pi_k^{cc}(g(n))$  for even  $k \geq 2$ , then  $L_f \in \Lambda_k(g(n))$ .*

The proof is by showing that there exists a family of languages such that a nondeterministic verification scheme can simulate a nondeterministic communication protocol. The theorem partially explains why it is difficult to separate the different levels of the local decision hierarchy – the question is inherently tied to long-standing open questions in communication complexity [1].

**Proof of Theorem 19.** Let  $f$  be a boolean function on  $2n$  variables. We will construct an infinite family of graphs  $\mathcal{G}_n = (G(n, t, x, y))_{t, x, y}$  and a related language  $L_f$ .

The graph  $G(n, t, x, y)$  consists of a path  $P_{2t+1} = (v_1, v_2, \dots, v_{2t+1})$  of length  $2t + 1$ , and two sets of nodes,  $V_A$  and  $V_B$  of size  $n$ . Let us denote  $v_A = v_1$  and  $v_B = v_{2t+1}$ . We add an edge between each  $v \in V_A$  and  $v_A$ , and an edge between each  $u \in V_B$  and  $v_B$ . The nodes  $v_A$  and  $v_B$  are labelled with their respective identities.

Parameters  $x$  and  $y$  are bit vectors of length  $n$ , corresponding to the inputs of players  $A$  and  $B$  in the communication complexity setting. To encode the input vectors, we use graphs on  $V_A$  and  $V_B$ , respectively. There are  $2^n$  possible input vectors. We'll define a function  $\phi$  that maps each graph on  $n$  nodes to an  $n$ -bit vector. Since the encoding of the input cannot depend on the unique identifiers,  $\phi$  must map all graphs of the same isomorphism class to the same vector. Finally, since there are at least  $2^{\binom{n}{2}}/n! = \Omega(2^{n^2})$  such graph isomorphism classes, we can find a  $\phi$  such that for all  $x \neq y$ , we have that  $\phi^{-1}(x) \cap \phi^{-1}(y) = \emptyset$ .

Given  $\phi$ ,  $x$ , and  $y$ , we can choose two graphs  $G_A \in \phi^{-1}(x)$  and  $G_B \in \phi^{-1}(y)$ , identify the node sets  $V_A$  and  $V_B$  with  $V(G_A)$  and  $V(G_B)$ , respectively, and add the corresponding edges to the graph  $G(n, t, x, y)$ . We will use  $G_A$  and  $G_B$ , respectively, to denote these graphs on node sets  $V_A$  and  $V_B$ . Nodes  $v_A$  and  $v_B$  are labelled as special nodes so that the structure of  $G_A$  and  $G_B$  can be detected. We denote this graph construction by  $G(n, t, x, y)$ .

**Local verification of  $\mathcal{G}_f$ .** A single  $O(\log n)$ -bit certificate is enough to verify the structure of  $G(n, t, x, y)$ . It first consists of a spanning tree of  $P_{2t+1}$ : node  $v_A$  is marked as root, and each node  $v_i$  has a pointer to  $v_{i-1}$  and a counter  $i$ , its distance to the root. It also contains the value  $n$ . The nodes  $v_A$  and  $v_B$  can check that the sizes of the graph  $G_A$  and  $G_B$  are consistent with this value. They also check that there are no other outgoing edges from  $G_A$  and  $G_B$ . Nodes  $v_A$  and  $v_B$  can see all nodes of  $G_A$  and  $G_B$ , and determine their isomorphism classes, and compute  $x = \phi(G_A)$  and  $y = \phi(G_B)$ , respectively.

**Deciding  $L_f$ .** We say that  $G \in L_f$  if and only if

1. the structure of  $G$  is that of  $G(n, t, x, y)$  for some setting of the parameters, and
2. the function  $f$  evaluates to 1 on  $\phi(G_A) \cup \phi(G_B)$ .

Now assume that  $f$  is on the  $k$ th level of the communication complexity hierarchy with  $s = \Omega(\log n)$  bits of nondeterminism. We can use this implied protocol  $P$  to solve  $L_f$  on the  $k$ th level. If the graph structure is correct, the prover and disprover essentially simulate their counterparts from the communication complexity setting, and label *all* nodes on  $P_{2t+1}$  as if in  $P$ . Then  $v_A$  can simulate  $A$  and  $v_B$  can simulate  $B$ , accepting if and only if  $f(x, y) = 1$ . If the prover tries to deviate from this strategy, nodes can see that its labelling of  $P_{2t+1}$  is not constant, and reject. If the disprover tries to deviate, the prover can construct a certificate pointing to this error, and all nodes will accept. ◀

**Global proofs and communication complexity.** In the setting of global proofs we can show a slightly stronger theorem.

► **Theorem 20.** *For every boolean function  $f$  and every  $g(n) = \Omega(\log n)$  there exists a distributed language  $L_f$  such that  $L_f \in \Lambda_k^G(g(n))$ , for  $k \geq 1$  if and only if  $f$  is in the  $k$ th level of the communication complexity hierarchy with  $O(g(n))$  bits of nondeterminism, in particular  $f \in \Sigma_k^{\text{cc}}$  for  $k$  odd or  $f \in \Pi_k^{\text{cc}}$  for  $k$  even.*

In particular, this theorem implies that any collapse in the hierarchy for global certificates implies a collapse in the corresponding communication complexity hierarchy.

**Proof of Theorem 20.** We show that with respect to the language  $L_f$  defined in the proof of Theorem 19, the communication complexity model and the global verification model can simulate each other.

1. *Communication protocol implies a global verification protocol.* The proof proceeds essentially as in the proof of Theorem 19. Using  $O(t \log n)$  bits the global certificate can give the list of nodes on the path between  $v_A$  and  $v_B$ . If a node has degree 2, it must see its own name on this list. Nodes  $v_A$  and  $v_B$  can again locally verify the structure of  $G_A$  and  $G_B$  and recover  $x$  and  $y$ . Finally the prover and disprover follow the communication protocol  $P$  on instance  $(x, y)$ , allowing nodes  $v_A$  and  $v_B$  to simulate Alice and Bob.

2. *Global verification scheme implies a communication protocol.* Assume there is a  $k$ th level global verification scheme with  $g(n)$ -bit certificates for  $L_f$ .

Alice and Bob will simulate this scheme as follows. Construct a virtual graph  $G(x, y)$  consisting of three parts: the nodes  $v_A$  and  $v_B$ , a path  $P_{2t+1}$  of length  $2t + 1$  between them, and graphs  $H(x)$  and  $H(y)$  that are the first elements (in some order) of  $\phi^{-1}(x)$  and  $\phi^{-1}(y)$ , respectively. Finally, all nodes of  $H(x)$  are connected to  $v_A$  and all nodes of  $H(y)$  to  $v_B$ . Only Alice will know  $H(x)$  and only Bob  $H(y)$ .

This graph is in  $L_f$  if and only if  $f(x, y) = 1$ : the structure is exactly as in the definition of  $L_f$ .

Now the nondeterministic prover and disprover can simulate their counterparts in the global verification scheme. Alice and Bob accept if and only if the prover can force all nodes they control to accept. Thus the complexity is bounded by the complexity  $g(n)$  of the global verification scheme. ◀

---

## References

- 1 László Babai, Peter Frankl, and Janos Simon. Complexity classes in communication complexity theory. In *Proc. 27th Annual Symposium on Foundations of Computer Science (FOCS 1986)*, pages 337–347, 1986. doi:10.1109/SFCS.1986.15.
- 2 Jørgen Bang-Jensen and Gregory Gutin. *Digraphs - theory, algorithms and applications*. Springer, 2002.
- 3 Keren Censor-Hillel, Ami Paz, and Mor Perry. Approximate proof-labeling schemes. In *Structural Information and Communication Complexity - 24th International Colloquium, SIROCCO 2017, Porquerolles, France, June 19-22, 2017, Revised Selected Papers*, pages 71–89, 2017. doi:10.1007/978-3-319-72050-0\_5.
- 4 Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms, 3rd Edition*. MIT Press, 2009. URL: <http://mitpress.mit.edu/books/introduction-algorithms>.
- 5 Laurent Feuilloley and Pierre Fraigniaud. Survey of distributed decision. *Bulletin of the EATCS*, 119, 2016. URL: <http://bulletin.eatcs.org/index.php/beatcs/article/view/411/391>.
- 6 Laurent Feuilloley and Pierre Fraigniaud. Error-sensitive proof-labeling schemes. In *31st International Symposium on Distributed Computing, DISC 2017, October 16-20, 2017, Vienna, Austria*, pages 16:1–16:15, 2017. doi:10.4230/LIPIcs.DISC.2017.16.
- 7 Laurent Feuilloley, Pierre Fraigniaud, and Juho Hirvonen. A Hierarchy of Local Decision. In *Proc. 43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016)*, volume 55 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 118:1–118:15, 2016. doi:10.4230/LIPIcs.ICALP.2016.118.
- 8 Pierre Fraigniaud, Amos Korman, and David Peleg. Local distributed decision. In *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*, pages 708–717, 2011. doi:10.1109/FOCS.2011.17.



- 9 Pierre Fraigniaud, Amos Korman, and David Peleg. Towards a complexity theory for local distributed computing. *J. ACM*, 60(5):35, 2013. doi:10.1145/2499228.
- 10 Mika Göös, Toniann Pitassi, and Thomas Watson. The landscape of communication complexity classes. In *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy*, pages 86:1–86:15, 2016. doi:10.4230/LIPIcs.ICALP.2016.86.
- 11 Mika Göös and Jukka Suomela. Locally checkable proofs in distributed computing. *Theory of Computing*, 12(1):1–33, 2016. doi:10.4086/toc.2016.v012a019.
- 12 Tom Gur and Ron D. Rothblum. Non-interactive proofs of proximity. In *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science, ITCS 2015, Rehovot, Israel, January 11-13, 2015*, pages 133–142, 2015. doi:10.1145/2688073.2688079.
- 13 Amos Korman and Shay Kutten. Distributed verification of minimum spanning trees. *Distributed Computing*, 20(4):253–266, 2007. doi:10.1007/s00446-007-0025-1.
- 14 Amos Korman, Shay Kutten, and David Peleg. Proof labeling schemes. In *Proceedings of the Twenty-Fourth Annual ACM Symposium on Principles of Distributed Computing, PODC 2005, Las Vegas, NV, USA, July 17-20, 2005*, pages 9–18, 2005. doi:10.1145/1073814.1073817.
- 15 Amos Korman, Shay Kutten, and David Peleg. Proof labeling schemes. *Distributed Computing*, 22(4):215–233, 2010. doi:10.1007/s00446-010-0095-3.
- 16 Elias Koutsoupias and Christos H. Papadimitriou. Worst-case equilibria. *Computer Science Review*, 3(2):65–69, 2009. doi:10.1016/j.cosrev.2009.04.003.
- 17 Fabian Kuhn. *The price of locality: exploring the complexity of distributed coordination primitives*. PhD thesis, ETH Zurich, 2005. URL: <http://d-nb.info/977273725>.
- 18 Eyal Kushilevitz and Noam Nisan. *Communication complexity*. Cambridge University Press, 1997.
- 19 László Lovász and Katalin Vesztegombi. Non-deterministic graph property testing. *Combinatorics, Probability & Computing*, 22(5):749–762, 2013. doi:10.1017/S0963548313000205.
- 20 Rafail Ostrovsky, Mor Perry, and Will Rosenbaum. Space-time tradeoffs for distributed verification. In *Structural Information and Communication Complexity - 24th International Colloquium, SIROCCO 2017, Porquerolles, France, June 19-22, 2017, Revised Selected Papers*, pages 53–70, 2017. doi:10.1007/978-3-319-72050-0\_4.
- 21 Christos H. Papadimitriou. Algorithms, games, and the internet. In *Proceedings on 33rd Annual ACM Symposium on Theory of Computing, July 6-8, 2001, Heraklion, Crete, Greece*, pages 749–753, 2001. doi:10.1145/380752.380883.
- 22 Boaz Patt-Shamir and Mor Perry. Proof-labeling schemes: Broadcast, unicast and in between. In *Stabilization, Safety, and Security of Distributed Systems - 19th International Symposium, SSS 2017, Boston, MA, USA, November 5-8, 2017, Proceedings*, pages 1–17, 2017. doi:10.1007/978-3-319-69084-1\_1.