Local certification of local properties: tight bounds, trade-offs and new parameters

Nicolas Bousquet, Laurent Feuilloley, Sébastien Zeitoun

Local certification of local properties: tight bounds, trade-offs and new parameters

Nicolas Bousquet
Univ Lyon, CNRS, INSA Lyon, UCBL, LIRIS, UMR5205 F-69622 Villeurbanne, France

Laurent Feuilloley
Univ Lyon, CNRS, INSA Lyon, UCBL, LIRIS, UMR5205, F-69622 Villeurbanne, France

Sébastien Zeitoun
Univ Lyon, CNRS, INSA Lyon, UCBL, LIRIS, UMR5205, F-69622 Villeurbanne, France

Abstract

Local certification is a distributed mechanism enabling the nodes of a network to check the correctness of the current configuration, thanks to small pieces of information called certificates. For many classic global properties, like checking the acyclicity of the network, the optimal size of the certificates depends on the size of the network, n. In this paper, we focus on properties for which the size of the certificates does not depend on n but on other parameters.

We focus on three such important properties and prove tight bounds for all of them. Namely, we prove that the optimal certification size is: $\Theta(\log k)$ for k-colorability (and even exactly $\lceil \log k \rceil$ bits in the anonymous model while previous works had only proved a 2-bit lower bound); $(1/2)\log t + o(\log t)$ for dominating sets at distance t (an unexpected and tighter-than-usual bound) ; and $\Theta(\log \Delta)$ for perfect matching in graphs of maximum degree Δ (the first non-trivial bound parameterized by Δ). We also prove some surprising upper bounds, for example, certifying the existence of a perfect matching in a planar graph can be done with only two bits. In addition, we explore various specific cases for these properties, in particular improving our understanding of the trade-off between locality of the verification and certificate size.

2012 ACM Subject Classification Theory of computation → Distributed algorithms

Keywords and phrases Local certification, local properties, proof-labeling schemes, locally checkable proofs, optimal certification size, colorability, dominating set, perfect matching, fault-tolerance, graph structure

Funding This work is supported by the ANR grant GrR (ANR-18-CE40-0032).

Acknowledgements The authors thank anonymous reviewers for useful comments.

1 Introduction

Local certification. Local certification is a topic at the intersection of locality and fault-tolerance in distributed computing. Very roughly, the main concern is to measure how much information the nodes of a network need to know in order to verify that the network satisfies a given property. Local certification originates from self-stabilization and is tightly related to the minimal memory needed to be sure that a self-stabilizing algorithm has reached a correct configuration locally. The topic is now studied independently, and the area has been very active during the last decade. We refer to the survey [14] for an introduction to the topic.

The standard model for local certification is the following. The nodes are first assigned labels, called *certificates*, and then every node looks at its certificate and the certificates of its neighbors, and decides to accept or reject. A certification scheme for a given property is correct if, for any network, the property is satisfied if and only if there exists a certificate assignment such that all the nodes accept. (We discuss variations later, and give proper definitions in Section 3.) The usual measure of performance of a certification scheme is the maximum certificate size over all nodes, and all networks of a given size.

One of the fundamental results in local certification is that any property can be certified if the network is equipped with unique identifiers [21, 20], but this is at the expense of huge certificates. Indeed, the scheme consists in giving to every node the full map of the graph, which takes $\Theta(n^2)$ bits in n-node graphs. The question then is: when can we do better? There exist three typical certificate sizes. For some properties, *e.g.* related to graph isomorphism, $\Theta(n^2)$ bits is the best we can do [20]. For many natural properties, the optimal certificate size is $\Theta(\log n)$; for example most properties related to trees (acyclicity, spanning tree, BFS, and minimum spanning tree for small edge weights [21]). A recent research direction tries to capture precisely which properties have such *compact certification* (see [4, 19, 18]). Finally, some properties are *local* from the certification point of view, in the sense that the optimal certification size *does not depend on* n. This third type of property is the topic of this paper.

Local certification of local properties. Until recently, studying local properties has not been the focus of the community, since the usual parameter for measuring complexity is the network size. A recent paper by Ardévol Martínez, Caoduro, Feuilloley, Narboni, Pournajafi and Raymond [22] is the first to target this regime. We refer to [22] for the full list of motivations to study this topic, and we just highlight a few points here.

First, it will appear in this paper that the size of the certificates for local properties is often expressed as functions of parameters different from the number of nodes. Therefore, one should not (always) see these are constants. It has been highlighted before (see discussion before Open problem 4 in [14]) that we have basically no understanding of certification size expressed by other parameters than the number of nodes.

Second, *locally checkable languages* (LCL) are at the core of the study of the LOCAL and CONGEST models. These are basically the properties that are local from a certification point of view: the output can be checked by looking at all the balls of some constant radius. Certification is a way to question the encoding of LCLs. A typical example is coloring, for which one uses the colors as output of a construction algorithm, and as certificates for colorability certification. If there would exist a better certification, this would shed a new light on the encoding of this LCL. For example, the celebrated round elimination technique [25] is very sensitive to the problem encoding, and one could hope that feeding it with a different encoding could provide new bounds. In a more general perspective, we argue that just like understanding the complexity of LCLs, understanding certification of local properties is a fundamental topic.

In addition to these two general motivations, our work is guided by two open problems, the k-colorability question and the trade-off conjecture, that we detail now.

The k-colorability question. Let us first discuss the case of colorability, which will be central in this paper. The property we want to certify is that the graph is *k-colorable*, that is, one can assign colors from $\{1, \dots, k\}$ to vertices such that no two neighbors have the same color. It is straightforward to design a local certification with k certificates for this property: the certificates encode colors in $\{1, \dots, k\}$ and the nodes just have to check that there is no conflict.[1] This uses $O(\log k)$ bits. The natural open problem here is the following.

▶ **Open problem 1** (Open problem 1 in [14]). *Is $\Theta(\log k)$ optimal for k-colorability certification?*

The first result on that question is the very recent paper [22] which establishes that one bit is not enough to certify k-colorability. This lower bound holds in the anonymous and in the proof-labeling scheme models, that we will define later. In a nutshell, the technique is an indistinguishability argument: assuming that there exists a 1-bit certification, one can argue about the number of 1s in a node neighborhood and take an accepting certification of some k-colorable graph to derive an accepting certification of a $k+1$-clique, which is a contradiction.

Interestingly, [22] also shows a case where the natural encoding is not the best certification. Namely, certifying a distance-2 3-coloring can be done with only 1 bit, while the obvious encoding of the colors takes 2 bits. Finally, let us mention that non-k-colorability, the complement property, is much harder to certify. Indeed, it is proved in [20] that one needs $\tilde{\Omega}(n^2)$ bits to certify non-3-colorability (where $\tilde{\Omega}$ hides inverse logarithmic factors).

Trade-off conjecture. We finish this general introduction, with yet another motivation to study local properties. The *trade-off conjecture*, first stated in [15], basically states that for any property, if the optimal certification size is s for the classic certification mechanism, where the nodes see their neighbors certificates, then it is in $O(s/d)$ if the vertices are allowed to see their whole neighborhood at distance d. This was proved to be true for many classic properties, and in many large graph classes [15, 17, 24]. Implicitly, the big-O of the conjecture refers to functions of n, but for local properties, the conjecture is interesting only if it refers to the parameters that appear in the certificate size.

▶ **Open problem 2** (Trade-off conjecture). *Consider a property with optimal certification size s at distance 1 (where s depends on the natural parameters of the problem). Is it true that if we allow the verification algorithm to look at distance d, then the optimal size is at most $\alpha \cdot s/d$ for some constant α?*

The authors of [22] argue that the conjecture might actually be wrong for local properties. In other words, there might exist properties such that looking further in the graph is useless (unless you can see the whole graph), or at least not as useful as claimed in [15] (instead of being s/d the optimal size could be a less-decreasing function of d). We consider this question to be very intriguing and important to the study of locality, and we will discuss it several times in the paper.

A sample of local properties. Local properties have different behaviors, which prevented us to establish general theorems capturing all of them. Instead, we looked for a sample of

[1] A *conflict* being an edge whose two endpoints are colored the same.

properties widely studied in the distributed community having diverse behaviors, and such that many other properties would behave similarly to one of the sample. First, we chose to study the colorability question, for the reasons cited above. Second we looked at domination at distance t, where a set of nodes is selected, and we want to check that every node is at distance at most t from a selected node. This property has inputs and an external parameter, which makes it very different from colorability. Moreover, a dominating set distance t is a building block for many self-stabilizing algorithms. Third, we study the property of "having a perfect matching". This differs from the two first ones by being an edge-related problem instead of the node-related problem, and it appears that the key parameter there is the maximum degree, a new parameter for certification. One more motivation is that matchings are classic objects in distributed graph algorithms.

Organization of the paper. The paper is organized the following way. After this introduction, we give a detailed overview of the context, results. We also give the proof techniques of the main results. Then, after a definition section, there are three technical sections that correspond to the three local properties we study. The overview and the technical parts can be read independently. Readers interested in motivations, general discussions, proof ideas and comparison with previous techniques can read the first and cherry-pick specific proofs they are curious about in the second; while others will prefer to go directly to the model section and formal proofs. The overview and the technical part are organized in the same way to allow easy back-and-forth reading.

2 Overview of our results and techniques

Quick description of the models

In order to state the results, we need to informally define the different models of certification (see Section 3 for more formal definitions).

- In the anonymous model, the nodes have no identifiers/port-numbers.
- In the proof-labeling scheme model, every node has a unique identifier (encoded on $O(\log n)$ bits) but it cannot access the identifiers of the other nodes.
- In the locally checkable proof model, nodes have identifiers and can see the identifiers of the other nodes.

The anonymous model is the one for which we have the largest number of results. It is usually less considered in the literature, but argue that for local properties it is the most natural. See the discussion in Subsection 3.2.

The standard assumption is that the nodes can only see their neighbors. Since we are interested in the trade-off conjecture, we will also consider certification at distance d, where the view is the full neighborhood at distance d.

It is often handy to say that the certificates are given by a *prover*, that intuitively tries to convince the nodes that the network is correct (both on correct and incorrect instances).

Now that we are equipped with these notions, we will review our results and techniques, problem by problem.

2.1 Overview for colorability

In this subsection, we consider the *k-colorability* property, already mentioned, which states that the graph is k-colorable.

Two lower bounds for colorability

We have already discussed the colorability property, and cited Open problem 1. Our first result is in the anonymous model, where we strongly solve Open problem 1 by determining the *exact bound*: in the anonymous model it is necessary and sufficient to have k different certificates.

▶ **Theorem 3.** *For every $k \geqslant 2$, in the anonymous model where vertices can see at distance 1, k certificates are needed in order to certify that a graph is k-colorable. Therefore, in the anonymous model, exactly $\lceil \log(k) \rceil$ bits are needed to certify k-colorability.*

The upper bound is trivial since we can simply give the colors as certificates. The technique to establish this lower bound is a form of crossing technique. We take a large enough complete k-partite graph, thus a graph that is maximally k-colorable, in the sense that any edge added to it would make it non-k-colorable. The idea of the proof is to argue by counting, that for any certificate assignment that would make all nodes accept this graph, there must exist two edges that we can cross (that is replace $(a, b); (x, y)$ by $(a, x); (b, y)$ for example) such that all neighborhoods appearing in this instance did appear in the previous one, thus no node rejects. In addition, the graph obtained after this crossing is non-k-colorable, which is a contradiction with the correctness of the scheme.

Now in the most general model, we also give an (asymptotic) tight bound, fully answering Open question 1. We actually prove a more general lower bound parametrized by the verification distance.

▶ **Theorem 4.** *In the locally checkable proofs model, at least $\Omega(\log(k)/d)$ bits are needed to certify k-colorability when the vertices are allowed to see their neighborhoods at distance d.*

We describe the proof of this result in a communication complexity framework to provide more intuition, although the actual proof does not rely on any black-box result from communication complexity. The instances we use have the typical shape of communication complexity constructions: the graph has two parts that correspond to the players (left and right) and a part in the middle. The middle part has a large diameter (to be sure that left and right cannot communicate at distance d), and has two sets of k special vertices on the left (top left and bottom left), and two sets of k special vertices on the right (top right and bottom right). The part of the left (resp. right) player is an antimatching between the top left and bottom left (resp. top right and bottom right), where an antimatching is a complete bipartite graph in which a matching has been removed. The middle part has a very constrained structure whose role is to enforce that the graph is k-colorable, if and only if, the left and right antimatchings are intuitively mirrors one of the other. The idea is then that the information about the exact matchings on the left and right parts has to be transferred to some node, to be compared, and this can happen only via the certificates. There are $k!$ possible forms for the left and right antimatchings, (because there are $k!$ possible matching in a complete bipartite graph of size k basically). Thus, the information that has to be transferred from one side of the graph to the other has size $k \log k$ (via Stirling equivalent) and since our graph has cuts of order k, we get the $\Omega(\log k)$ lower bound.

Uniquely k-colorable graphs and other natural counterexample candidates

Our two lower bound constructions have in common to be very constrained, in a precise sense: for every vertex v, every ball centered in v of radius at least 2 admits a unique proper k-coloring (up to color renaming). In this case, we say that the graph is *uniquely k-colorable*

at distance d (where d is the radius of the neighborhood). It is easy to see that if a graph is uniquely k-colorable at distance d, then either it has a unique k-coloring or it is not k-colorable. Intuitively, graphs with this property are hard for certification, since there is no slack in the coloring, thus the transfer of information between different parts of the graph cannot a priori be compressed. Perhaps surprisingly, we prove that for these graphs the trade-off conjecture does hold, even in the anonymous model.

▶ **Theorem 5.** *For every $d \leqslant \log k$, in the anonymous model where vertices can see at distance d, $O(\log k/d)$ bits are sufficient to certify that a uniquely k-colorable graph at distance $d-2$ is k-colorable.*

Let us briefly explain the main ingredient of that proof. Since the coloring is locally unique, by looking far enough, a node can decide which other nodes are in the same color class in a k-coloring, if one exists globally. This is not enough to be sure that the graph is k-colorable, because the color classes might not coincide nicely. For example, every cycle is uniquely 2-colorable at distance 1, but this does not certify that the full cycle is 2-colorable. The key idea is that a node will recover the name of its color by gathering the bits of information spread on the nodes *of its own color class* at distance at most d from it. This allows to spread the information of the color classes on several vertices and then use smaller certificates. Slightly more formally, the certifier will assign to a well-chosen subset of nodes X a special certificate. The vertices of X are chosen far enough from each other so that we can store information of the different color classes on the nodes close to it. But they are also chosen not too far away from each other to be sure that all the vertices are close to a vertex of X. Now every node just have to perform the following verification: (i) if it is too far from any vertex of X, it rejects, (ii) it checks that its color is the same for all vertices of X close to it, (iii) it checks that for all the vertices of X close to it, the color associated to it is different from colors given to its neighbors.

After Theorem 5, a question is whether we can go down to a constant number of bits, or in other words, how large the constant of the big-O needs to be. We prove that at a distance $O(\log k)$, *one bit is sufficient* (in other words only two different certificates are needed). Note that it means in particular that we can avoid the special certificate of the proof of Theorem 5 by being very careful on how we represent each vertex of X and the colors classes around it (and proving that even if a node makes a mistake in the choice of X when some vertices are indistinguishable, its decision will be anyway correct).

▶ **Theorem 6.** *In the anonymous model where vertices can see to distance d, 2 certificates are enough to certify that a uniquely k-colorable graph at distance $d-2$ is k-colorable, if $d \geqslant 9\lceil \log_2 k \rceil + 8$.*

The scheme for this is built on the same framework, but with more ideas and technicalities, and we refer to the technical part for the details.

Now that we proved that locally uniquely colorable graphs are not going to help, we wonder what would be a good candidate to disprove the trade-off conjecture (of course one might not exist, if the conjecture is true). We believe that for graphs that are *almost* locally uniquely colorable (that is, they have few correct colorings locally, up to color renaming) the proof of Theorem 5 could be adapted, with more layers of technicalities. Hence, one might go for graphs that have *many* possible colorings. This could make sense from a communication complexity point of view, because there also exist difficult problems with many correct pairs of inputs (*e.g.* the disjointness problem). What is problematic here is that unlike in communication complexity, in our case, on a k-colorable graph, the prover has the choice of the coloring, thus can choose one that is easier to encode compactly.

Since graphs that are very structured seem to admit a linear scaling, another approach could be to consider graphs with a more chaotic structure. Random graphs are natural candidates here, but even if we could come up with a satisfying definition for what it means to certify the colorability of a random graph, it is not clear that this would be hard. Indeed, there exist efficient algorithms to k-color k-colorable graphs (*e.g.* [27]) that exploit only the local structure of the graph, so one could even hope for a verification without certificates.

In the end, graphs with large girth and large chromatic number might be the right type of graphs to consider because they have both a large number of colorings locally and a rigid structure globally. Several constructions for these have been designed (see *e.g.* [13, 23, 9]), but they are randomized or complex, which makes their study rather challenging.

Certification versus output encoding

More generally, it is interesting to explore the links between (1) certifying that a given structure exists (*e.g.* a coloring here, but also a perfect matching a bit later in the paper) (2) explicitly describing it, and (3) implicitly describing it, that is giving enough information to recover the structure, but not directly (*e.g.* with fewer bits than the natural encoding). We refer to [3] for the related topic of distributed zero-knowledge proofs.

For colorability, the case of perfect graphs is a nice example of the discrepancy that can exist between these. A graph is *perfect* if its chromatic number is equal to the size of its maximum clique for every induced subgraph. Many classic graph classes are perfect, *e.g.* bipartite graphs, chordal graphs, comparability graphs (see [26] for a survey on perfect graphs). If we are promised to be in such a graph, the verification (at distance 2) is very easy: a vertex just has to check whether it belongs to a clique of size larger than k (in which case it rejects, otherwise it accepts). Thus, no certificates are needed for colorability certification, while it seems really difficult to have the nodes output a coloring without giving them quite a lot of information. Proving formally such a discrepancy would be a nice result.

Finally, let us mention yet another lower bound approach, related to problem encodings. One can note that if we have certification using s bits for a property, where the local verification algorithm runs in polynomial time in the network size, then we have a *centralized* decision algorithm for this property in time $s^n\text{poly}(n)$. Indeed, one can just enumerate all the possible certificate assignments of this size and check whether one is accepted. One could hope that having a too-good bound for certification would imply that some big conjecture (*e.g.* SETH, the strong exponential hypothesis) is wrong, and get a conditional lower bound.[2] Unfortunately, this does not help us much for certification, since there are known algorithms for computing the chromatic number of a graph in time $O(c^n)$ with $c < 3$ (*e.g.* in [6]).

2.2 Overview for domination

The *domination at distance t* property applies to graphs with inputs: every node should be labeled with 0 or 1, and every node should be at distance at most t from a node labeled 1. To avoid confusion, let us highlight that in the domination property, the inputs are part of the instance and are different from the certificates.

This problem is quite different from colorability, in several ways. First, it is a problem that is centered on inputs: for any graph there are inputs that are correct, so in some sense it is the inputs that are certified more than the graph itself. (This is actually closer to the

[2] Such bounds are not common in certification, but not unseen, see [11].

original self-stabilizing motivation of certifying the output of an algorithm.) Second, the natural certification has a different flavor: we give every node its distance to the closest node of the dominating set (that is, a node labeled 1), and every node checks that these distances do make sense. One can then consider domination at distance t to be the local analogue of acyclicity, which is certified by providing the nodes of the network with the distance to the root.

Given this analogy with acyclicity, a $\Theta(\log t/d)$ optimal certificate size is expected, and indeed we prove it. But we go one step further by providing precise bounds on the number of different certificates. First, for the anonymous model at distance 1, we prove that the optimal number of different certificates is basically $\sqrt{t}$.

▶ **Theorem 7.** *Let $t \in \mathbb{N}^*$. In the anonymous model where vertices can see to distance 1, at least $\sqrt{t-1}$ different certificates are needed to certify a dominating set at distance t, even if the graphs considered are just paths and cycles.*

The lower bound is again quite expected: the proof for this kind of bound is based on arguing whether the same pair of certificates can appear several times on a path or not, thus the square root pops up naturally.

▶ **Theorem 8.** *In the anonymous model where vertices can see to distance 1, $3 \cdot \lceil \sqrt{t} \rceil$ certificates are sufficient to certify a dominating set at distance t.*

This upper bound is more surprising. It reveals that the natural encoding (consisting of giving the minimum distance to a labeled vertex) is not the best, and that the square root is not an artifact of the lower bound proof but is necessary. The proof of Theorem 8 is based on an elegant argument using *de Bruijn words*. Roughly, for some parameters k and n, a de Bruijn word is a (cyclic) word on an alphabet of size k, which contains all the factors (that is subwords of consecutive letters) of size n exactly once. The idea here is that instead of giving the certificate r to nodes at distance r from a node labeled 1, we will give them the r-th letter in a predefined de Bruijn word that corresponds to $n = 2$ and $k = \sqrt{t}$. Since every node will see its neighbors' certificates, thus a factor of size at least 2, it will be able to decode what is its position in the word, thus its distance to the 1-labeled node. The parametrization $k = \sqrt{t}$ ensures that the de Bruijn word of the correct length exists. Finally, we generalize these bounds to larger distances using generalizations of the techniques described above.

▶ **Theorem 9.** *In the anonymous model where vertices can see to distance $d < \frac{t}{2}$, at least $\sqrt[2d]{t-2d+1}$ different certificates are needed to certify a dominating set at distance t, even if the graphs considered are just paths and cycles.*

▶ **Theorem 10.** *In the anonymous model where vertices are allowed to see to distance d, $O(\sqrt[d+1]{t})$ certificates are sufficient to certify a dominating set at distance t.*

2.3 Overview for perfect matchings

A graph has the *perfect matching property* if it has a perfect matching, that is, a set of edges such that every vertex belongs to exactly one such edge. It is yet another type of property, that differs from the others by the fact that it has no built-in parameter (no number k of colors, or distance t). As we will see, the relevant parameter here is the maximum degree of the graph.

Perfect matching certification upper bounds

The natural way to locally encode a matching in distributed computing is to make every node know which port number corresponds to a matched edge (if the vertex is matched). In the port-number model, this directly leads to a certification: give the relevant port number to each node, and let them check the consistency. This takes $O(\log \Delta)$ bits per node, but it requires port numbers, and the ability for the nodes to know the port numbers of their neighbors.

Our first result is that we do not need port-numbers (nor any kind of initial symmetry-breaking). The strategy for the prover is the following. First, choose a perfect matching, and color the matched edges such that there are no two edges (u, v) and (w, z) of the same color with (v, w) being an edge of the graph. We call this a *matching coloring*. Then, give to every node the color of its matched edge. Then every node simply checks that it has exactly one neighbor with the same color.

▶ **Theorem 11.** *Let $k \in \mathbb{N}^*$. Let $\mathcal{C}$ be a class of graphs such that, for every $G \in \mathcal{C}$, if G has a perfect matching then G has a k-matching coloring. Then, in the anonymous model at distance 1, k certificates are enough to certify the existence of a perfect matching in G for every $G \in \mathcal{C}$.*

We can easily show (Lemma 28) that if G has a perfect matching then it admits a $(2\Delta - 1)$-matching coloring.

▶ **Corollary 12.** *For every graph G, $2\Delta - 1$ certificates are enough to certify the existence of a perfect matching, in the anonymous model at distance 1.*

To better appreciate the lower bound of the next paragraph, let us mention a surprising result on the upper bound side. Note first that if we can get a matching coloring using fewer colors, then we automatically get a more compact certification. Now consider a planar graph with an arbitrary perfect matching. We claim that this perfect matching can be colored with only four colors, even though planar graphs can have an arbitrary large maximum degree. Indeed, if we contract the edges of the matching, we still have a planar graph, and we can color this graph with four colors, by the four color theorem. Now undoing the contraction, and giving to the matched edges the color of their contracted vertices, we get a proper matching coloring with only four colors. We also prove a more general result on minor-free and bounded treewidth graphs.

▶ **Corollary 13.** *In the anonymous model at distance 1:*

- *Only 2 bits are enough to certify the existence of a perfect matching for planar graphs.*
- *Only $O(\log k)$ bits are needed to certify the existence of a perfect matching in K_k-minor-free graphs.*
- *Only $\lceil \log_2(k+1) \rceil$ bits are needed to certify the existence of a perfect matching in graphs of treewidth at most k.*

Note that, all our upper bounds follow from the existence of k-matching colorings. One can easily remark that, if instead of certifying a perfect matching one is simply interested in representing and certifying a matching, we can also do it with the same method by simply coloring all the unmatched vertices with an additional color. Since all the graph classes we mention in the upper bounds are closed under vertex deletion, our results ensure that the following holds: We can represent and certify matchings with 2Δ certificates for general graphs, 5 certificates for planar graphs and $t + 2$ certificates for graphs of treewidth at most t.

Perfect matching certification lower bounds

We prove the following lower bound for perfect matching certification.

▶ **Theorem 14.** *For every $\Delta \geqslant 2$, in the anonymous model where vertices can see at distance 1, Δ different certificates are needed to certify the existence of a perfect matching for graphs of maximum degree Δ.*

Before we sketch the proof, let us note that there is no natural candidate for a lower bound: on the one hand, graphs that are sparse are ruled out by Corollary 13, and on the other hand many dense graph classes are known to always have perfect matchings, *e.g.* even cliques, or even random graphs with at least $n \log n$ edges [12].

The key to the proof is the notion of *half-graphs*. Half-graphs are bipartite graphs with vertices $u_1, ..., u_n$ and $v_1, ..., v_n$ such that u_i is linked to $v_1, ..., v_i$. In such a graph, there exists a *unique* perfect matching, and it uses the edges (u_i, v_i). Indeed, u_1 must be matched with v_1, thus u_2 must be matched with v_2 etc. Now, we prove by counting argument that if such a graph is accepted with fewer than Δ certificates, we can create a graph without perfect matching that is also accepted. The idea is to take two copies of this certified graph, and then to carefully remove edges from within these graphs to add edges in between. Again, we refer to the technical section for the details.

Discussion of the parameter Δ

A remarkable feature of the perfect matching property is that the optimal certificate size is completely captured by the maximum degree (if we do not consider restricted graph classes). As far as we know, it is the first time that Δ appears as a natural parameter for local certification. This is interesting, since there are few results that use graph parameters other than the size of the graph to measure certificate size. To our knowledge, the only pure graph parameter that has been used before and that does not appear as a parameter of the problem is the girth, for approximate certification [11].[3] It has been highlighted, *e.g.* in [14] (discussion before open problem 5), that developing a theory of parametrized certification is an interesting research direction.

Let us note however that it is maybe not very surprising that the maximum degree appears as a key parameter for matching-related problems, since celebrated papers have proved that it is central to the complexity of such problems in other models of computation, *e.g.* the LOCAL model [1, 5].

3 Model and definitions

3.1 Graphs

All the graphs we consider are finite, simple, and non-oriented. For completeness, let us recall the following classical graph definitions. Let $G = (V, E)$ be a graph, $u, v \in V$, $S \subseteq V$, $i \in \mathbb{N}$. The *distance between u and v*, denoted by $d(u, v)$, is the length (number of edges) of the shortest path from u to v. The *layer at distance i from u*, denoted by $N^i(u)$, is the set of vertices $v \in V$ such that $d(u, v) = i$. The *ball of radius i centered in u*, is $B(u, i) := \bigcup_{0 \leqslant j \leqslant i} N^j(u)$. The *closed (resp. open) neighborhood* of u is $N[u] := B(u, 1)$ (resp. $N^1(u)$). We can similarly define $d(u, S), N(S)$ and $N[S]$ when S is a subset of vertices.

[3] The maximum edge weight also appears for problems in weighted graphs, *e.g.* minimum spanning tree [21], max-weight matching [20, 7].

3.2 Certification

Let $G = (V, E)$ be a graph, and let C, I be non-empty sets. A *certificate function of* G (with certificates in C) is a mapping $c : V \to C$. An *identifier assignment of* G (with identifiers in I) is an injective mapping $Id : V \to I$.

▶ **Definition 15.** *Let c be a certificate function of G and Id be an identifier assignment of G. Let $u \in V$, $d \in \mathbb{N}^*$. The* view of u at distance d *consists in all the information available at distance at most d from u, that is:*

- *the vertex u;*
- *the graph with vertex set $B(u, d)$ and the edges $(v_1, v_2) \in E(G)$ such that $\{v_1, v_2\} \cap B(u, d-1) \neq \emptyset$;*
- *the restriction of c to $B(u, d)$;*
- *the restriction of Id to $B(u, d)$.*

▶ Remark 16. For a vertex u, the subgraph induced by $B(u, d-1)$ is included in the view of u at distance d. However, the subgraph induced by $B(u, d)$ is *not* included in the view of u at distance d in general (because the view of u does not contain the edges between two vertices v_1 and v_2 which are both at distance exactly d from u).

A *verification algorithm (at distance d) in the locally checkable proof model* is a function which takes as input the view (at distance d) of a vertex, and outputs a decision, *accept* or *reject*. For a property $\mathcal{P}$ on graphs, we say that there is a *certification for* $\mathcal{P}$ using k certificates (resp. k bits) if C has size k (resp. 2^k), and if there exists a verification algorithm A such that for every graph G and every identifier assignment Id, G has property $\mathcal{P}$ if and only if there exists a certificate function c such that A accepts for every $v \in V(G)$.

A *verification algorithm in the anonymous model* is defined in the exact same way that a verification algorithm in the locally checkable proof model, but vertices are not equipped with a unique identifier (or equivalently, the output is invariant with respect to the identifier assignment).

In this paper, we do not use the proof-labeling scheme model, where the node has access only its own ID, but it appears in a relevant previous work [22].

Discussion of the anonymous model

Note that the model we chose as our main model is the anonymous one. Indeed, all our results are for this model, except for the lower bound on colorability which we wanted to strengthen to the model with identifiers in order to fully solve Open Problem 1.

We think that the natural model for local properties is anonymous. Indeed, the main reason why identifiers are common in local certification is that they are often necessary, which is not the case for local properties. For example, certifying tree-like structures requires certifying that there is a unique connected component, and for this identifiers are needed. Note that in the LOCAL model, identifiers are also used to break symmetry, but in certification, the certificates can do this.

Moreover, the anonymous model is very common in the self-stabilizing literature (see *e.g.* [16, 2, 8]) which is the origin of local certification.

Third, in the paper, we draw a parallel between certification of local properties and LCLs, and the identifiers do not appear in the definition of LCLs.

Finally, in the cases known in the literature where anonymous and "with-ID" bounds match (*e.g.* acyclicity), the proofs are similar in spirit, except that the ID case involves

more counting arguments (usually assuming that the ID interval is not of linear size), which implies loosing constants everywhere, getting results that are less crisp, and proofs that are more obfuscated.

4 Colorability certification

In this section, we will consider the certification of the *k-colorability* property. Let us recall that a graph G is said to be k-colorable if there exists *proper k-coloring* of G, that is, is a mapping $\varphi : V \to \{1, \dots k\}$ such that for all $(u, v) \in E$, $\varphi(u) \neq \varphi(v)$.

For completeness, let us start by proving the following simple upper bound.

▶ **Proposition 17.** *In the anonymous model where vertices can see at distance 1, k-colorability can be certified with $\lceil \log k \rceil$ bits.*

Proof. For a graph $G = (V, E)$ which is k-colorable, the certificate function given by the prover is the following. The prover chooses a proper k-coloring φ of G, and assigns certificate $c(u) := \varphi(u)$ to every $u \in V$. The verification algorithm of every vertex u consists in checking if for every neighbor v, $c(u) \neq c(v)$. If it is the case, u accepts. Otherwise, u rejects. It is clear that the graph is accepted if and only if it is k-colorable. ◀

4.1 Lower bounds

▶ **Theorem 3.** *For every $k \geqslant 2$, in the anonymous model where vertices can see at distance 1, k certificates are needed in order to certify that a graph is k-colorable. Therefore, in the anonymous model, exactly $\lceil \log(k) \rceil$ bits are needed to certify k-colorability.*

Proof. Assume by contradiction that there exists a certification of k-colorability in the anonymous model using only $k-1$ different certificates. The idea of the proof is to consider a specific k-colorable graph G_k, for which there must exist an accepting certification function. We will prove that we can flip (*i.e.* cross) two edges of G_k such that the resulting graph G'_k is not k-colorable and no vertex is able to detect it (meaning that the local view of each vertex will be unchanged). Thus, in the new graph G'_k, each vertex accepts, which is a contradiction since G'_k is not k-colorable.

Let us denote by G_k the complete k-partite graph, where each set has size $\max(k, 3)$. More formally, let $V_1, \dots, V_k$ be k disjoint sets, each of size $\max(k, 3)$. Let G_k be the graph with vertex set $V = \bigcup_{i=1}^{k} V_i$ where (u, v) is an edge if and only if u and v do not belong to the same set V_i. Since $\{V_1, \dots, V_k\}$ is a partition of V into k independent sets, G_k is k-colorable. Thus, by hypothesis, there exists a certificate function $c : V \to \{1, \dots, k-1\}$ such that every vertex accepts. By the pigeonhole principle, for every $i \in \{1, \dots, k\}$ there exist two different vertices $u_i, v_i \in V_i$ such that $c(u_i) = c(v_i)$ (since each set has size at least k). Again, by the pigeonhole principle, there exist $i \neq j$ such that $c(u_i) = c(u_j)$. Thus, we get $c(u_i) = c(v_i) = c(u_j) = c(v_j)$, with $u_i, v_i \in V_i$ and $u_j, v_j \in V_j$. Let G'_k be the graph obtained from G_k by removing the two edges $(u_i, u_j), (v_i, v_j)$ and adding the two edges $(u_i, v_i), (u_j, v_j)$, as depicted on Figure 1.

We claim that, with the same certificate function c, all the vertices of G'_k accept. Indeed, the only vertices whose neighborhood have been modified between G_k and G'_k are u_i, v_i, u_j, v_j. So every vertex in $V \setminus \{u_i, v_i, u_j, v_j\}$ accepts. For u_i, the only difference between its neighborhood in G_k and G'_k is that u_j is replaced by v_i. Since $c(u_j) = c(v_i)$, the view of u_i is the same in G_k and G'_k, so u_i accepts in G'_k as well. Similarly, one can prove that v_i, u_j, and v_j accept in G'_k.

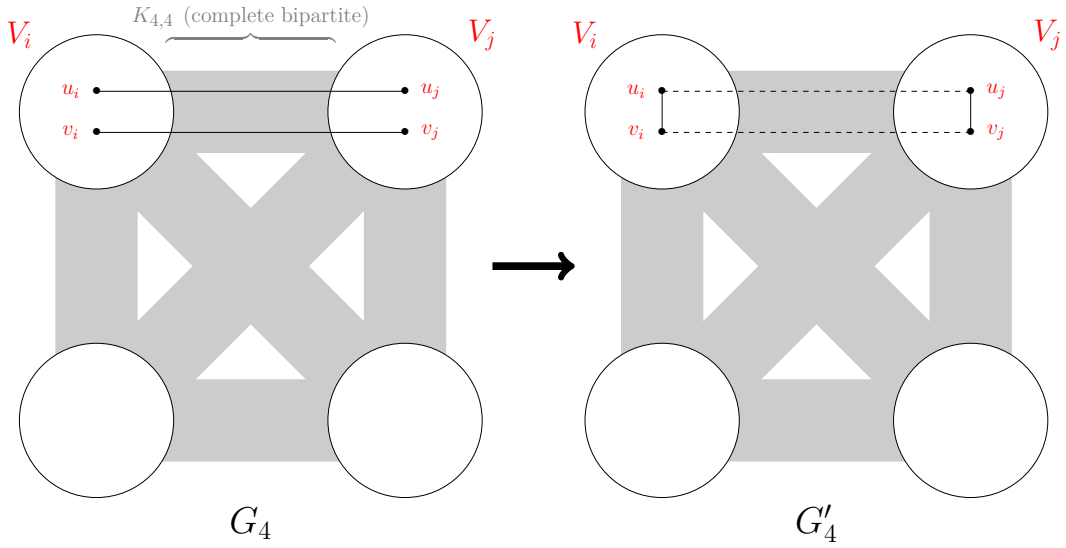

Figure 1 Our constructions for the proof of Theorem 3, in the case of $k = 4$. The gray strips indicate complete bipartite graphs. The edges we are interested in appear explicitly.

However, G'_k is not k-colorable. Indeed, assume by contradiction that it is, and let φ be a proper k-coloring of G'_k. For any $r \notin \{i, j\}$, let $w_r \in V_r$. Let w_j be a vertex of $V_j \setminus \{u_j, v_j\}$ which exists, since each set contains at least 3 vertices. Then, $K = \{w_1, \ldots, w_{i-1}, w_{i+1}, \ldots w_k\}$ is a clique in G'_k, so the $(k-1)$ vertices of K receive pairwise different colors in φ. Moreover, both u_i and v_i are complete to K. So if G'_k is k-colorable, then u_i and v_i have to be colored the same, which is a contradiction since $(u_i, v_i) \in E(G'_k)$. ◀

Obtaining lower bounds is usually harder in the locally checkable proofs model. In this more demanding model, we do not get the exact bound in terms of number certificates, but still we get a bound that would be considered optimal by the usual standards. Namely, we will prove that $\Omega(\log k)$ bits are needed to certify the k-colorability of a graph. More generally, we prove that, if vertices can see their neighborhoods at distance d, at least $\Omega(\log k/d)$ bits are needed to certify k-colorability. Note that the graph constructed in the proof of Theorem 3 has diameter two, thus no lower bound at distance at least 3 can be obtained from that construction. The lower bound of the following theorem is obtained with a completely different graph.

▶ **Theorem 4.** *In the locally checkable proofs model, at least $\Omega(\log(k)/d)$ bits are needed to certify k-colorability when the vertices are allowed to see their neighborhoods at distance d.*

Proof. For $r, s \geqslant 2$, let us denote by $P_{r,s}$ the graph on vertex set $V = \{1, \ldots, r\} \times \{1, \ldots, s\}$ with the following edges:

- for all $i \neq j \in \{1, \ldots, r\}$ and all $p \in \{1, \ldots, s\}$, $((i, p), (j, p)) \in E$
- for all $i \neq j \in \{1, \ldots, r\}$ and all $p \in \{1, \ldots, s-1\}$, $((i, p), (j, p+1)) \in E$

In other words, the graph $P_{r,s}$ is a sequence of s cliques $\mathcal{K}_1, \ldots, \mathcal{K}_s$, each having size r, with an antimatching[4] between $\mathcal{K}_i$ and $\mathcal{K}_{i+1}$ for all $i \leqslant s-1$. The second coordinate indicates

[4] Remember that an antimatching between two sets of nodes is an edge set containing all the possible edges between the two sets, except for a matching.

the index of the clique the vertex belongs to, and for all (i,p) with $p \leqslant s-1$, (i,p) is the only vertex in $\mathcal{K}_p$ which is not adjacent to $(i,p+1)$. For instance, the graph $P_{3,5}$ is depicted on Figure 2.

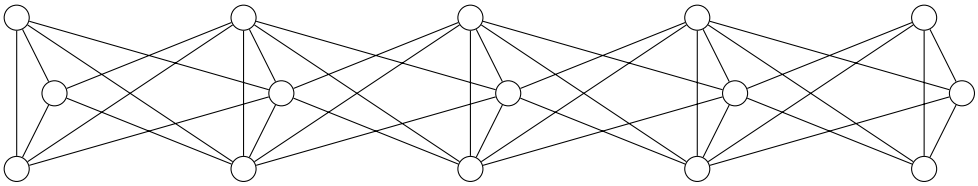

Figure 2 The graph $P_{3,5}$. Here the cliques are triangles, and two consecutive cliques are linked by all possible edges except for the horizontal ones (the antimatching).

Now, for any pair of permutations σ, τ of $\{1,\dots,r\}$, let us denote by $G_{r,s}(\sigma,\tau)$ the graph obtained in the following way. We take two copies of $P_{r,s}$, and we denote their cliques by $\mathcal{K}_1,\dots,\mathcal{K}_s$ and $\mathcal{K}'_1,\dots,\mathcal{K}'_s$. We give $2rs$ different identifiers to the vertices of the two copies (the identifiers are fixed, they do not depend on σ and τ). Finally, we add the antimatching $\{(i,\sigma(i))\}_i$ between $\mathcal{K}_1$ and $\mathcal{K}'_1$, and the antimatching $\{(i,\tau(i))\}_i$ between $\mathcal{K}_s$ and $\mathcal{K}'_s$ (see Figure 3 for an illustration).

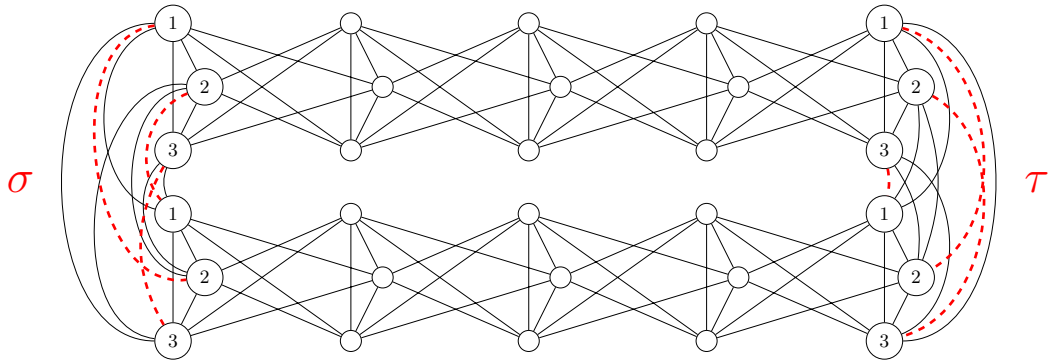

Figure 3 The graph $G_{3,5}(\sigma,\tau)$, where σ is the permutation $(1,2)$ and τ the cycle $(1,2,3)$.

▷ Claim 18. The graph $G_{r,s}(\sigma,\tau)$ is r-colorable if and only if $\sigma = \tau$.

Proof. Since $\mathcal{K}_1$ is a clique of size r, in a proper coloring with r colors, every color appears exactly once inside $\mathcal{K}_1$. Similarly, every color appears exactly once in a proper coloring of $\mathcal{K}_2$. For all $i \in \{1,\dots,r\}$, the vertex $(i,1)$ is a neighbor of every vertex in $\mathcal{K}_2$ except $(i,2)$. Thus, the vertices $(i,1)$ and $(i,2)$ are colored the same. Hence, given a coloring of $\mathcal{K}_1$, there exists a unique way to properly color $\mathcal{K}_2$. This propagates along the cycle of cliques $\mathcal{K}_2,\dots\mathcal{K}_s,\mathcal{K}'_s,\dots,\mathcal{K}'_1$, and it leads to a proper coloring of the whole graph if and only if the coloring of $\mathcal{K}'_1$ is compatible with the coloring of $\mathcal{K}_1$, that is, if and only if $\sigma = \tau$. ◀

Using Claim 18, we will deduce a lower bound on the number of bits needed to certify k-colorability, when vertices are allowed to see at distance d. We consider the construction above with parameters $r = k$ and $s = 2d$. Assume that m bits are sufficient. Then, for any permutation σ, there exists a certificate function $c_\sigma : V \to \{0,\dots,2^m-1\}$ such that all the vertices of $G_{k,2d}(\sigma,\sigma)$ accept. Suppose that there are two different permutations σ,τ such that the certification functions are the same: $c_\sigma = c_\tau$, that is, all vertices receive the same certificate in both instances. Then $G_{k,2d}(\sigma,\tau)$ would be accepted with this certificate

function, since the view of every vertex would be identical as its view in $G_{k,2d}(\sigma,\sigma)$ (for vertices in the left part) or in $G_{k,2d}(\tau,\tau)$ (for vertices in the right part). This would be a contradiction because $G_{k,2d}(\sigma,\tau)$ is not k-colorable (by Claim 18).

Hence, all the certificate functions c_σ are different. In particular, there are no more permutations of $\{1,\dots,k\}$ than functions $V \to \{0,\dots,2^m-1\}$. The set V has size $4kd$ since it is made of two copies of a graph of size $k \times 2d$. Therefore, we get $k! \leqslant 2^{4mkd}$, leading to $m \geqslant \frac{\log_2(k!)}{4kd}$. Finally, since $\log_2(k!) = \Omega(k \log k)$, we get the result. ◀

▶ Remark 19. Two ingredients of the proof, the communication complexity insight and the antimatchings to propagate the coloring, have already been used in [20], to get a lower bound on the certification of not-3-colorable graphs.

4.2 Upper bounds: uniquely colorable graphs

We can wonder if the lower bound of Theorem 4 can be improved and be independent of d. We will show that if it is the case, it is impossible with graphs similar to the ones used to prove Theorem 4. Indeed, these graphs have a strong property which can be exploited to get an almost tight upper bound: all the balls of radius $d \geqslant 2$ are uniquely colorable, up to the permutation of color classes. This property, that allowed us to control how the coloring can be transmitted and helped us to obtain the lower bound, can also be used to improve the upper bound. Let us first formally define uniquely colorable graphs.

▶ **Definition 20.** *Let $k, n \in \mathbb{N}$. A graph G is* uniquely k-colorable at distance d *if, for every vertex v, the graph induced by $B(v,d)$ is uniquely k-colorable up to the permutation of the color classes.*

One can easily note that, for every $r \geqslant 1, s \geqslant 3$, and for all permutations σ, τ of $\{1,\dots,r\}$, the graphs $G_{r,s}(\sigma,\tau)$ introduced in the proof of Theorem 4 are uniquely r-colorable at distance 2. Note moreover that every graph G that is uniquely k-colorable at distance d is either uniquely k-colorable at distance $d+1$, or has a ball of radius $d+1$ which is not k-colorable.

Before proving the main statements of this section, let us first give some properties satisfied by uniquely k-colorable graphs:

▶ **Lemma 21.** *Let $k, d \in \mathbb{N}$. For every uniquely k-colorable graph G at distance d which is (globally) k-colorable, every color α and every vertex u, the following holds:*

(i) at least one vertex of color α appears in $N[u]$;
(ii) for every $i \in \mathbb{N}$, at least one vertex of color α appears at distance i, $i+1$ or $i+2$ from u (if $N^{i+2}(u) \neq \emptyset$).

Proof. Let G be a uniquely k-colorable graph at distance d, u be a vertex and α be a color.

(i) Assume by contradiction that color α does not appear in the closed neighborhood of u. Then, we can obtain another proper coloring by changing the color of u to α, which is a contradiction since G is uniquely k-colorable.
(ii) Let v be a vertex at distance $i+1$ from u. By applying (i) to v, there exists a vertex $w \in N[v]$ of color α, and w is at distance i, $i+1$ or $i+2$ from u. ◀

We are now ready to state and prove the following theorem.

▶ **Theorem 5.** *For every $d \leqslant \log k$, in the anonymous model where vertices can see at distance d, $O(\log k/d)$ bits are sufficient to certify that a uniquely k-colorable graph at distance $d-2$ is k-colorable.*

Proof. We actually prove the following more precise result in the model where vertices are allowed to see at distance $d \geqslant 11$. Let $\delta := \left\lfloor \frac{d-2}{9} \right\rfloor$ and $f(k) := \left\lceil \sqrt[\delta]{k} \right\rceil$. Note that $\delta \geqslant 1$, and that every integer in $\{0, \dots k-1\}$ needs at most δ digits to be represented in base $f(k)$. Let us prove that $f(k)+1$ certificates are sufficient to certify k-colorability for uniquely k-colorable graphs at distance $d-2$. (The theorem follows by taking the logarithm of this quantity.) The set of certificates we will use is $\{0, 1, \dots, f(k)\}$.

Let $G = (V, E)$ be a uniquely k-colorable graph at distance $d-2$ which is k-colorable. Let us denote by φ a proper k-coloring of G using colors $\{0, \dots, k-1\}$. The prover gives the following certificates. The prover first chooses a maximal independent set X at distance $6\delta+1$, and gives to all the vertices $u \in X$ the certificate $c(u) := f(k)$. Then, for every vertex $v \in V \setminus X$ such that $d(v, X) \leqslant 3\delta$, let $i_v := \left\lceil \frac{d(v,X)}{3} \right\rceil$. The certificate $c(v)$ given by the prover to v is the i_v-th digit of the decomposition of $\varphi(v)$ in base $f(k)$. Note that $c(v) \neq f(k)$. Finally, the prover gives to all the vertices at distance at least $3\delta+1$ from X an arbitrary certificate in $\{0, \dots, f(k)-1\}$. Intuitively, the name of the color is encoded on the vertices of that color, the first bit on a first circular strip (of thickness three: the vertices at distance 1, 2 and 3 from the vertex in X), the second bit on a second circular strip, etc.

The informal idea of the verification is the following. Since X is a maximal independent set at distance $6\delta+1$, each vertex v should see at least one vertex $u \in X$ at distance $6\delta \leqslant d-2$. Since G is uniquely colorable, v will determine the set of vertices around u which are in its color class, and will then determine its own color thanks to their certificates. Finally, v will compare its color to the color of its neighbors.

Let us now formalize this intuition. Every vertex $v \in V$ checks its certificate as follows. If the diameter of the connected component of v is at most 6δ, then v sees its whole connected component and accepts if and only if it is k-colorable. Otherwise, let us denote by X the set of vertices with certificate $f(k)$. The vertex v performs the following verification steps:

(i) v starts by checking if $B(v, 6\delta) \cap X \neq \emptyset$. If it is not the case, then v rejects.

(ii) Let $u \in B(v, 6\delta) \cap X$. Since $d \geqslant 9\delta+2$, $B(v, d-2)$ contains $B(u, 3\delta)$. Since $B(v, d-2)$ is uniquely colorable, v determines the color classes $\mathcal{C}_1, \dots, \mathcal{C}_k$ of $B(v, d-2)$. Let us denote by $\mathcal{C}_\ell$ the color class of v. For every $i \in \{1, \dots, \delta\}$, v checks if all the vertices in $\mathcal{C}_\ell \cap (N^{3i-2}(u) \cup N^{3i-1}(u) \cup N^{3i}(u))$ have the same certificate. If it is not the case, v rejects. Otherwise, let us denote by a_i this common certificate. Note that a_i is well-defined. Indeed, since the connected component of v has diameter at least $6\delta+1$, $N^j(u) \neq \emptyset$ for all $j \leqslant 3\delta$. And Lemma 21 ensures that at least one vertex of $\mathcal{C}_\ell$ appears in every three consecutive layers around u. Let $a(v, u)$ be the integer whose decomposition in base $f(k)$ is $a_1 \dots a_\delta$.

(iii) Then, v checks if, for every pair of vertices $u, u' \in B(v, 6\delta) \cap X$, we have $a(v, u) = a(v, u')$. If it is not the case, v rejects. Otherwise, let us denote by $a(v)$ this common value. If $a(v) \notin \{0, \dots, k-1\}$, then v rejects.

(iv) For every $w \in N(v)$, v can determine $a(w)$. Indeed, $a(w)$ only depends on $B(w, d-2)$ which is included in $B(v, d-1)$. So it is in the view of v. If $a(w) = a(v)$ for some $w \in N(v)$, then v rejects.

(v) If v did not reject at this point, then v accepts.

To conclude, we simply have to show that a uniquely k-colorable graph at distance $d-2$ is accepted with this verification algorithm if and only if it is k-colorable. If a graph G is k-colorable, then the above checking algorithm indeed accepts with the certificates given by the prover as described above. Conversely, if all the vertices accept, then we can construct a proper k-coloring of G by giving to each vertex v the color $a(v)$. It uses at most k colors

because of step (iii). Moreover, it is a proper coloring since step (iv) ensures that every vertex v is colored differently from all its neighbors. ◀

▶ Remark 22. Unique colorability can also be tested by the verification algorithm (instead of making the assumption that the input graph is uniquely colorable). In other words, there is a certification using the same number of certificates, which accepts the input graph if and only if it is a uniquely k-colorable graph at distance $d-2$ which is k-colorable.

One can wonder how much we can decrease the number of certificates when d increases. We prove that we can decrease it up to 2 (which is the best one could hope for). To do so, the main difficulty is that, in the proof of Theorem 5, we used a special certificate (namely the certificate $f(k)$) to certify the vertices of the maximal independent set X, and then at least 2 other certificates to code the colors. We will show that we can get rid of the special certificate, by modifying the certification around the vertices of X.

▶ **Theorem 6.** *In the anonymous model where vertices can see to distance d, 2 certificates are enough to certify that a uniquely k-colorable graph at distance $d-2$ is k-colorable, if $d \geqslant 9\lceil \log_2 k \rceil + 8$.*

Proof. Let $\delta = \lceil \log_2 k \rceil$. We will prove that, in the model where vertices can see at distance $d = 9\delta + 8$, only 2 certificates are sufficient in order to certify that a uniquely k-colorable graph at distance $d-2$ is k-colorable. In the following, we denote these two certificates by 0 and 1.

On a graph $G = (V, E)$ which is k-colorable, the prover gives the following certificates. Let us denote by φ a proper k-coloring of G using colors $\{0, \dots, k-1\}$. The prover begins by choosing a maximal independent set X at distance $6\delta + 5$, and gives to all the vertices $u \in X$ the certificate 1. He also gives certificate 1 to all the vertices v such that $d(v, X) = 1$, and certificate 0 to all the vertices v such that $d(v, X) = 2$. For every vertex v such that $3 \leqslant d(v, X) \leqslant 3\delta + 2$, let $i_v := \left\lceil \frac{d(v,X)-2}{3} \right\rceil$. The certificate $c(v)$ given by the prover to v is the i_v-th digit of the decomposition of $\varphi(v)$ in base 2. Finally, the prover gives certificate 0 to all the vertices v such that $d(v, X) \geqslant 3\delta + 3$.

A vertex $v \in V$ checks its certificate as follows. If the diameter of the connected component of v in G is at most $6\delta + 4$, then v sees its whole connected component and accepts if and only if it is k-colorable. Otherwise, let us denote by Y the set of vertices u such that (a) $c(u) = 1$ and, (b) $c(u') = 1$ for all $u' \in N(u)$ and, (c) $c(u') = 0$ for all $u' \in N^2(u)$. The vertex v performs the following verification steps:

(i) v starts by checking if $B(v, 6\delta + 4) \cap Y = \emptyset$. If it is the case, then v rejects.
(ii) Let $u \in B(v, 6\delta + 4) \cap Y$. Since $d = 9\delta + 8$, $B(v, d-2)$ contains $B(u, 3\delta + 2)$. Since $B(v, d-2)$ is uniquely colorable, v determines the color classes $\mathcal{C}_1, \dots, \mathcal{C}_k$ of $B(v, d-2)$. Let us denote by $\mathcal{C}_\ell$ the color class of v. For every $i \in \{1, \dots, \delta\}$, v checks if all the vertices in $\mathcal{C}_\ell \cap (N^{3i}(u) \cup N^{3i+1}(u) \cup N^{3i+2}(u))$ have the same certificate. If it is not the case, v rejects. Otherwise, let us denote by a_i this common certificate. As in proof of Theorem 5, a_i is well-defined by Lemma 21. Let $a(v, u)$ be the integer whose decomposition in base 2 is $a_1 \dots a_\delta$.
(iii) Then, v checks if, for every pair of vertices $u, u' \in B(v, 6\delta+4) \cap Y$, we have $a(v, u) = a(v, u')$. If it is not the case, v rejects. Otherwise, let us denote by $a(v)$ this common value. If $a(v) \notin \{0, \dots, k-1\}$, then v rejects.
(iv) For every $w \in N(v)$, v can determine $a(w)$. Indeed, $a(w)$ only depends on $B(w, d-2)$ which is included in $B(v, d-1)$. So it is in the view of v. If $a(w) = a(v)$ for some $w \in N(v)$, then v rejects.

(v) If v did not reject at this point, then v accepts.

To conclude, we have to show that a uniquely k-colorable graph at distance $d-2$ is accepted with this verification algorithm if and only if it is k-colorable. If all the vertices accept, we construct a proper k-coloring of the graph by giving to each vertex v the color $a(v)$. It uses at most k colors because of step (iii) and it is a proper coloring because step (iv) ensures that every vertex v is colored differently from all its neighbors.

Conversely, assume that a graph G is k-colorable. We need to show that every vertex accepts with the certificate function given by the prover as described before. It is more difficult than in proof of Theorem 5, since we have $X \subseteq Y$ but we may not have the equality. Hence, some vertices in $Y \setminus X$ can lead some vertex to reject at step (iii). We will prove that it cannot happen because of the following claim:

▷ Claim 23. With the certificate function given by the prover, every vertex $y \in Y \setminus X$ is a twin of some vertex $x \in X$ (that is $N[y] = N[x]$).

Proof. Let us consider the certificates assigned by the prover, and let $y \in Y \setminus X$. Let us denote by x the closest vertex in X from y. By construction, we have $X \subseteq Y$, so $x \in Y$. First, let us prove that $d(x,y) = 1$. Assume by contradiction that $d(x,y) \geqslant 2$. We distinguish some cases depending on $d(x,y)$:

- $d(x,y) = 2$. Since $y \in Y$, we get $c(x) = 0$. But $x \in Y$, so it should have certificate 1, which is a contradiction.
- $d(x,y) = 3$. Then, there exists $w \in N^2(y) \cap N(x)$. This is a contradiction, since $y \in Y$ implies that $c(w) = 0$ and $x \in Y$ implies that $c(w) = 1$.
- $4 \leqslant d(x,y) \leqslant 3\delta + 2$. By Lemma 21, there is a vertex $z \in N[y]$ colored by 0. Note that $d(z,X) \geqslant 3$.
  If $d(z,X) \leqslant 3\delta + 2$, then the certificate of z given by the prover is a digit of the decomposition of its color in base 2. Since z is colored by 0, z has certificate 0.
  If $d(z,X) \geqslant 3\delta + 3$, then z has certificate 0 by construction.
  So y has a neighbor with certificate 0, which is a contradiction since $y \in V$.
- $d(x,y) \geqslant 3\delta + 3$. Then, y has certificate 0 by construction and y cannot be in Y.

So $d(x,y) = 1$. Let us finally prove that x and y are twins. We prove that $N(y) \setminus \{x\} = N(x) \setminus \{y\}$. Let $z \in N(y) \setminus \{x\}$. Since $y \in Y$, we get $c(z) = 1$. Moreover, $d(x,z) \in \{1,2\}$ since $d(x,y) = 1$. Since $x \in Y$, we cannot have $d(x,z) = 2$ since otherwise this would imply $c(z) = 0$. Thus, $d(x,z) = 1$, so $z \in N(x) \setminus \{y\}$. Thus, $N(y) \setminus \{x\} \subseteq N(x) \setminus \{y\}$. By symmetry, we get the other inclusion. So x and y are twins, which completes the proof of Claim 23. ◀

We can now conclude the proof of Theorem 6. In the way the prover assigned certificates, every vertex v will see at least one vertex $u \in Y$ at distance at most $6\delta + 4$. It will then compute $a(v,u)$. But since u is either in X or a twin of a vertex $w \in X$, u and w has the same neighborhoods at distance d for every $d \geqslant 2$. Thus, $a(v,u) = a(v,w)$. Then, by construction, every vertex v will accept. ◀

5 Dominating sets at large distance

In this section, we consider *labeled* graphs: every graph G is equipped with a label function $\mathcal{L} : V(G) \to \{0,1\}$ which is part of the input (in other words, the certificate function given by the prover depends on the label function). We say that a vertex v is *labeled* if $\mathcal{L}(v) = 1$. We focus on the number of certificates needed to certify that the set of labeled vertices is a

dominating set at distance t (we remind that a dominating set at distance t is a set $S \subseteq V$ such that $\cup_{v \in S} B(v,t)$ is equal to V).

5.1 Lower bounds

▶ **Theorem 7.** *Let $t \in \mathbb{N}^*$. In the anonymous model where vertices can see to distance 1, at least $\sqrt{t-1}$ different certificates are needed to certify a dominating set at distance t, even if the graphs considered are just paths and cycles.*

Proof. Let us denote by P_{t+1} the path having $t+1$ vertices denoted by $u_0, \ldots, u_t$, where only u_0 is labeled. Note that $\{u_0\}$ is a dominating set at distance t in P_{t+1} (see Figure 4 for an illustration).

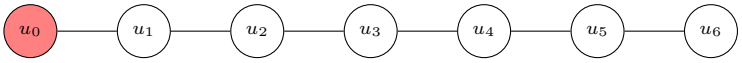

Figure 4 The graph P_7.

Since P_{t+1} is a valid instance, there exists a certificate function c such that every vertex accepts. Let us prove that for $1 \leqslant i < j \leqslant t-1$, the pairs of certificates $(c(u_i), c(u_{i+1}))$ and $(c(u_j), c(u_{j+1}))$ must be distinct. Assume by contradiction that it is not the case, and let $i < j$ such that $(c(u_i), c(u_{i+1})) = (c(u_j), c(u_{j+1}))$. Let us prove that, for every possible pair (i,j), we can find a graph G that is accepted and should not be. There are several cases:

- if $j = i+1$, we get $c(u_i) = c(u_{i+1}) = c(u_{i+2})$. Thus, the triangle where all the vertices receive the certificate $c(u_{i+1})$ is accepted, since the view of every vertex of the triangle is the same as the view of u_{i+1} in P_{t+1}. But this graph should not be accepted since it does not contain any labeled vertex.
- if $j = i+2$, then the cycle of length 4 where the vertices receive successively the certificates $c(u_i)$ and $c(u_{i+1})$ is accepted, since every vertex has either the view of u_{i+1} or the view of u_{i+2} in P_{t+1}. But it should not be accepted since it does not contain any labeled vertex.
- if $j \geqslant i+3$, then the cycle of length $j-i$ where vertices have certificates $c(u_i)$, $c(u_{i+1}), \ldots,$ $c(u_{j-2}), c(u_{j-1})$ is accepted. Indeed, for every $\ell \in \{i+1, \ldots, j-1\}$, the vertex certified by $c(u_\ell)$ has the view of u_ℓ in P_{t+1}, and the vertex certified by $c(u_i)$ has the view of u_j in P_{t+1}. Again, this graph should not be accepted since it does not contain any labeled vertex.

Hence, all the pairs of certificates of consecutive vertices have to be pairwise distinct. Since we need at least $t-1$ different pairs of certificates, there must be at least $\sqrt{t-1}$ different certificates in P_{t+1}. ◀

We can wonder if the lower bound of Theorem 7 can be generalized when vertices are allowed to see at distance $d \leqslant t$. We will see that in Corollary 24 that the lower bound is in fact divided by d.

▶ **Theorem 9.** *In the anonymous model where vertices can see to distance $d < \frac{t}{2}$, at least $\sqrt[2d]{t-2d+1}$ different certificates are needed to certify a dominating set at distance t, even if the graphs considered are just paths and cycles.*

▶ **Corollary 24.** *In the anonymous model where vertices can see at distance $d \leqslant \frac{t}{3}$, $\Omega(\log(t)/d)$ bits are needed to certify a dominating set at distance t.*

Proof of Theorem 9. The proof generalizes the one of Theorem 7. As in the proof of Theorem 7, we consider the graph P_{t+1}. Since P_{t+1} has a dominating set at distance t, there exists a certificate function c such that every vertex accepts. Let us prove that $2d$-tuples of consecutive certificates $(c(u_i), \dots, c(u_{i+2d-1}))$ have to be pairwise distinct for every $i \in \{1, \dots, t-2d+1\}$. Assume by contradiction there exist $i < j$ such that $(c(u_i), \dots, c(u_{i+2d-1})) = (c(u_j), \dots, c(u_{j+2d-1}))$. Let $r = j - i$. The finite sequence $(c(u_i), c(u_{i+1}), \dots, c(u_{j+2d-1}))$ has its $2d$ first and last values equal, so it is r-periodic.[5] Let us consider the cycle C on $r \cdot (2d+1)$ vertices denoted by $v_0, \dots, v_{r(2d+1)-1}$ with no labeled vertex. The graph C does not have any labeled vertex, so it should not be accepted. However, let us show that it is accepted with some certificate function. For every $\ell \in \{0, \dots, r \cdot (2d+1) - 1\}$, the prover gives to the vertex v_ℓ the certificate $c(u_{i+d+(\ell \mod r)})$. We claim that every vertex accepts. Indeed, for every $\ell \in \{0, \dots, r \cdot (2d+1) - 1\}$, v_ℓ has the same view as $u_{i+d+(\ell \mod r)}$ in P_{t+1}. This is a contradiction.

Hence, at least $t - 2d + 1$ different $2d$-tuples of certificates are needed to certify P_{t+1}, so at least $\sqrt[2d]{t-2d+1}$ different certificates are needed. ◀

5.2 Upper bounds

In this subsection, we prove upper bounds matching with the previous lower bounds, thus giving the optimal bounds to certify a dominating set at large distance. Firstly, the lower bound of Theorem 7 is optimal up to a constant factor, as stated in the following Theorem 8, which shows that the optimal size is $\frac{\log t}{2} + o(\log t)$ if the vertices can see at distance 1.

▶ **Theorem 8.** *In the anonymous model where vertices can see to distance 1,* $3 \cdot \lceil \sqrt{t} \rceil$ *certificates are sufficient to certify a dominating set at distance* t*.*

Before proving Theorem 8, we will define a few notions. Let A be an alphabet, and $\omega, \omega' \in A^*$. We say that ω is a *factor* of ω' if there exists a sequence of consecutive letters in ω' which is equal to ω. Let us now define *de Bruijn words*, whose existence is well-known.

▶ **Proposition 25.** *Let* $k, n \in \mathbb{N}^*$*, and* A *be an alphabet of size* k*. There exists a word* $\omega \in A^*$ *of length* k^n*, such that every word of* A^n *appears at most once as a factor of* ω*. Such a word* ω *is called a* (k, n)-de Bruijn word.[6]

Proof of Theorem 8. Let $\tau = \lceil \sqrt{t} \rceil$. Let us prove that 3τ certificates are sufficient to certify a dominating set at distance t (in the anonymous model, where vertices can see at distance 1). Let $A := \{1, \dots, \tau\}$. The certificates used in the scheme will be pairs in $C := \{0, 1, 2\} \times A$. For $(x, y) \in C$, let $\pi_1(x, y) := x$ and $\pi_2(x, y) := y$. Let $\omega' \in A^*$ be a $(\tau, 2)$-de Bruijn word (which, by definition, has length at least t), and let us denote by $\omega = \omega_1 \dots \omega_t$ its prefix of length exactly t.

Let $G = (V, E)$ be a graph and $S \subseteq V$ be the set of labeled vertices. If S is dominating at distance t, the certificate function given by the prover is the following. The vertices of S are given an arbitrary certificate, and for every $u \in V \setminus S$ at distance i from S, the prover gives to u the certificate $c(u)$ which is $(i \mod 3,\ \omega_i)$.

---

[5] It is not necessarily a cyclic periodicity. By saying that this finite sequence is r-periodic, we mean that $c(u_k) = c(u_{k+r})$ for all $k \in \{i, \dots, i + 2d - 1\}$.

[6] Usually, de Bruijn words are defined as words of length k^n such that each word of A^n appears at least once when ω is considered circularly. But due to the length of ω, each word of A^n actually appears exactly once circularly, so at most once if ω is not seen as a circular word.

The informal idea of the verification is the following one. In its certificate, every vertex u is given a letter of ω. By looking at its neighbors, u will be able to determine its position in ω (since a pair of letters defines a unique position in the de Bruijn word ω), which corresponds to its distance to S.

More formally, let c be a certificate function. Each vertex u checks the certificate as follows :

(i) If $N[u] \cap S \neq \emptyset$, then u accepts.[7]
(ii) Else, u checks that, for all $u', u'' \in N[u]$, if $\pi_1(c(u')) = \pi_1(c(u''))$ then $\pi_2(c(u')) = \pi_2(c(u''))$. If it is not the case, u rejects.
(iii) Then, u checks if it has at least one neighbor v such that $\pi_1(c(v)) = \pi_1(c(u)) - 1 \mod 3$, and if $\pi_2(c(v))\pi_2(c(u))$ is a factor of ω. If it is not the case, u rejects.
(iv) Finally, for every neighbor w such that $\pi_1(c(w)) = \pi_1(c(u)) + 1 \mod 3$, u checks if ω has $\pi_2(c(v))\pi_2(c(u))\pi_2(c(w))$ as a factor. If it is not the case, then u rejects.
(v) If u did not reject at this point, it accepts.

It remains to show that there exists a certificate function such that all the vertices of G accept if and only if S is dominating at distance t. If S is a dominating set at distance t, then one can easily check that all the vertices accept with the certificates assigned by the prover as described previously. Note that with this certificate function, for step (ii), if $u', u'' \in N[u]$ satisfy $\pi_1(c(u')) = \pi_1(c(u''))$, then $d(u', S) = d(u'', S)$ so $\pi_2(c(u')) = \pi_2(c(u''))$.

For the converse, assume that G is accepted with some certificate function c. By (iii), every $u \in V$ such that no vertex is labeled in $N[u]$ should have a neighbor v such that $\pi_1(c(v)) = \pi_1(c(u)) - 1 \mod 3$ and $\pi_2(c(v))\pi_2(c(u)) = \omega_\ell\omega_{\ell+1}$ for some ℓ. Note that since ω is a de Bruijn word, this ℓ is unique. Let us prove by induction on $\ell \in \{1, \dots, t-1\}$ that $d(u, S) \leqslant \ell + 1$.

- For $\ell = 1$, we have $\pi_2(c(v))\pi_2(c(u)) = \omega_1\omega_2$. Let us prove that $d(u, S) \leqslant 2$. It is sufficient to prove that $d(v, S) \leqslant 1$. If v accepts at step (i), the conclusion holds. So we can assume that v accepts at step (v). By (iii), v has a neighbor v' such that $\pi_1(c(v')) = \pi_1(c(v)) - 1 \mod 3$ and $\pi_2(c(v'))\pi_2(c(v))$ is a factor of ω. Since v does not reject at step (iv), $\pi_2(c(v'))\pi_2(c(v))\pi_2(c(u))$ is a factor of ω. So the letters $\omega_1\omega_2 = \pi_2(c(v))\pi_2(c(u))$ appear at least twice as a factor of ω, which is a contradiction with the definition of de Bruijn words. Indeed, $\pi_2(c(v))\pi_2(c(u))$ are already the first two letters of ω. So if a factor $\pi_2(c(v'))\omega_1\omega_2$ appears somewhere, $\omega_1\omega_2$ must appear at least twice. Hence, v accepts at step (i), so $d(v, S) \leqslant 1$.
- Assume now that $\ell \geqslant 2$. To prove that $d(u, S) \leqslant \ell+1$, it is sufficient to prove that $d(v, S) \leqslant \ell$. If v accepts at step (i) the conclusion holds. So we can assume that v accepts at step (v). By (iii), v has a neighbor v' such that $\pi_1(c(v')) = \pi_1(c(v)) - 1 \mod 3$ and $\pi_2(c(v'))\pi_2(c(v))$ is a factor of ω. Since v does not reject at step (iv), $\pi_2(c(v'))\pi_2(c(v))\pi_2(c(u))$ is a factor of ω. Since the factor $\pi_2(c(v))\pi_2(c(u))$ appears exactly once in ω and $\pi_2(c(v))\pi_2(c(u)) = \omega_\ell\omega_{\ell+1}$, we have $\pi_2(c(v'))\pi_2(c(v)) = \omega_{\ell-1}\omega_\ell$ by (iv). By induction hypothesis, it implies that $d(v, S) \leqslant \ell$.

Thus, for any vertex $u \in V$, if u accepts at step (i) we have $d(u, S) \leqslant 1$, otherwise we have $d(u, S) \leqslant t$ by the previous induction. So S is indeed a dominating set at distance t. ◀

[7] We could verify that $\pi_2(c(u))$ corresponds to a letter in the beginning of ω, but it is not necessary.

In the case where vertices can see at distance $d \geqslant t$, we will see in Corollary 26 that the bound of Corollary 24 is also optimal: the number of bits is divided by d.

▶ **Theorem 10.** *In the anonymous model where vertices are allowed to see to distance d, $O(\sqrt[d+1]{t})$ certificates are sufficient to certify a dominating set at distance t.*

▶ **Corollary 26.** *In the anonymous model where vertices can see at distance d, $O(\log(t)/d)$ bits are sufficient to certify a dominating set at distance t.*

Proof of Theorem 10. The idea of the proof is similar to the one of Theorem 8.

Let $\tau = \lceil \sqrt[d+1]{t} \rceil$. Let us prove that 3τ certificates are sufficient to certify a dominating set at distance t (in the anonymous model, where vertices can see at distance d). Let $A = \{1, \dots, \tau\}$. The set of certificates that will be given to vertices consists of pairs in $C = \{0, 1, 2\} \times A$. For $(x, y) \in C$, let $\pi_1(x, y) := x$ and $\pi_2(x, y) := y$. Let $\omega' \in A^*$ be a $(\tau, d+1)$-de Bruijn word (which, by definition, has length at least t), and let us denote by $\omega = \omega_1 \dots \omega_t$ its prefix of length exactly t.

Let $G = (V, E)$ be a graph and $S \subseteq V$ be the set of labeled vertices. If S is a dominating set at distance t, the certificate function given by the prover is the following. Vertices of S are given an arbitrary certificate, and for every $u \in V \setminus S$ at distance i from S, the certificate $c(u)$ is $(i \mod 3, \omega_i)$.

The informal idea of the verification is the following one. In its certificate, every vertex u is given a letter of ω. By looking at its neighbors, u will be able to determine its position in ω, which corresponds to its distance to S.

More formally, let c be a certificate function. Each vertex u_0 checks the certificate as follows :

(i) If $B(u_0, d) \cap S \neq \emptyset$, then u_0 accepts.
(ii) Else, u_0 checks if there exists a path $u_0 u_1 \dots u_d$ such that $\pi_1(c(u_i)) = \pi_1(c(u_0)) - i \mod 3$ for every $i \in \{0, \dots, d\}$. Let us call such a path a *decreasing path (starting at u_0)*. If u_0 does not have any decreasing path, u_0 rejects.
(iii) Then, u_0 checks if $\pi_2(c(u_d)) \dots \pi_2(c(u_0))$ is the same for all the decreasing paths, and if it is a factor of ω. If it is not the case, u_0 rejects.
(iv) Finally, for every neighbor w such that $\pi_1(c(w)) = \pi_1(c(u_0)) + 1 \mod 3$, u_0 checks if ω has $\pi_2(c(u_d)) \dots \pi_2(c(u_0))\pi_2(c(w))$ as a factor. If it is not the case, then u_0 rejects.
(v) If u_0 did not reject at this point, it accepts.

It remains to show that there exists a certificate function such that all the vertices of G accept if and only if S is a dominating set at distance t. If S is a dominating set at distance t, then one can easily check that all vertices accept with the certificates assigned by the prover described previously. Note that with this certificate function, for step (iii), if $u_0 \dots u_d$ is a decreasing path, then $d(u_i, S) = d(u_0, S) - i$ for all $i \in \{0, \dots, d\}$, so $\pi_2(c(u_d)) \dots \pi_2(c(u_0))$ is a factor of ω.

For the converse, assume that G is accepted with some certificate function c. By (ii) and (iii), every $u_0 \in V$ such that no vertex is labeled in $B(u_0, d)$ should have a decreasing path $u_0 u_1 \dots u_d$, such that $\pi_2(c(u_d)) \dots \pi_2(c(u_0)) = \omega_\ell \dots \omega_{\ell+d}$ for some ℓ. Note that since ω is a de Bruijn word, this ℓ is unique. Let us prove by induction on $\ell \in \{1, \dots, t-d\}$ that $d(u_0, S) \leqslant \ell + d$.

- For $\ell = 1$, we have $\pi_2(c(u_d)) \dots \pi_2(c(u_0)) = \omega_1 \dots \omega_{d+1}$. Let us prove that $d(u_0, S) \leqslant d + 1$. It is sufficient to prove that $d(u_1, S) \leqslant d$. If u_1 accepts at step (i), the conclusion holds. So we can assume that u_1 accepts at step (v). By (ii) and (iii), there exists a decreasing

path $u_1v_1 \dots v_d$ (starting at u_1) such that $\pi_2(c(v_d)) \dots \pi_2(c(v_1))\pi_2(c(u_1))$ is a factor of ω. Since u_1 does not reject at step (iv), $\pi_2(c(v_d)) \dots \pi_2(c(v_1))\pi_2(c(u_1))\pi_2(c(u_0))$ is a factor of ω. Note that $u_0u_1v_1 \dots v_{d-1}$ is a decreasing path. Since u_0 does not reject at step (iii), we get $\pi_2(c(v_{d-1})) \dots \pi_2(c(v_1))\pi_2(c(u_1))\pi_2(c(u_0)) = \pi_2(c(u_d)) \dots \pi_2(c(u_0))$. Thus, the factor $\omega_1 \dots \omega_{\ell+1} = \pi_2(c(u_d)) \dots \pi_2(c(u_0))$ appears at least twice in ω, which is a contradiction. Hence, u_1 accepts at step (i), so $d(u_1, S) \leqslant d$.

- Assume now that $\ell \geqslant 2$. To prove that $d(u_0, S) \leqslant \ell + d$, it is sufficient to prove that $d(u_1, S) \leqslant \ell + d - 1$. If u_1 accepts at step (i) the conclusion holds. So we can assume that u_1 accepts at step (v). By (ii) and (iii), there exists a decreasing path $u_1v_1 \dots v_d$ (starting at u_1) such that $\pi_2(c(v_d)) \dots \pi_2(c(v_1))\pi_2(c(u_1))$ is a factor of ω. Since u_1 does not reject at step (iv), $\pi_2(c(v_d)) \dots \pi_2(c(v_1))\pi_2(c(u_1))\pi_2(c(u_0))$ is a factor of ω. Note that $u_0u_1v_1 \dots v_{d-1}$ is a decreasing path. Since u_0 does not reject at step (iii), then $\pi_2(c(v_{d-1})) \dots \pi_2(c(v_1))\pi_2(c(u_1))\pi_2(c(u_0)) = \pi_2(c(u_d)) \dots \pi_2(c(u_0))$. Since the factor $\pi_2(c(u_d)) \dots \pi_2(c(u_0))$ appears exactly once in ω and $\pi_2(c(u_d)) \dots \pi_2(c(u_0)) = \omega_\ell \dots \omega_{\ell+d}$, we have $\pi_2(c(v_d)) \dots \pi_2(c(v_1))\pi_2(c(u_1)) = \omega_{\ell-1} \dots \omega_{\ell+d-1}$ by (iv). By induction hypothesis, we get $d(u_1, S) \leqslant \ell + d - 1$ and then the conclusion holds.

Thus, for any vertex $u_0 \in V$, if u accepts at step (i) then $d(u, S) \leqslant d$, otherwise we have $d(u, S) \leqslant t$ by the previous induction. So S is indeed a dominating set at distance t. ◀

6 Perfect matchings

In this section, we will consider the certification of the existence of a *perfect matching*. Let us recall that a perfect matching of a graph G is a set $M \subseteq E(G)$ which satisfies the following property: for all $v \in V(G)$, there exists a unique $e \in M$ such that $v \in e$.

6.1 Upper bounds

In order to certify perfect matching, we will certify matching colorings which are defined as follows:

▶ **Definition 27.** *Let $G = (V, E)$ be a graph. A* k-matching coloring *of G is a mapping $\varphi : V \to \{1, \dots, k\}$ such that there exists a perfect matching M satisfying the following property: for every edge $(u, v) \in E$, $\varphi(u) = \varphi(v)$ if and only if $(u, v) \in M$.*

This is not the same definition as the one given in the introduction, but the two are equivalent.

For every graph G, we denote by $\Delta(G)$ (or simply Δ when G is clear from context) the maximum degree of G.

▶ **Lemma 28.** *Let $G = (V, E)$ be a graph with a perfect matching M. There exists a $(2\Delta - 1)$-matching coloring of G.*

Proof. We construct a $(2\Delta - 1)$-matching coloring φ of G as follows: we greedily color one after the other the edges of M. For an edge $(u, v) \in M$, u has at most $\Delta - 1$ neighbors different from v, and v has at most $\Delta - 1$ neighbors different from u, each of them being incident to at most one edge of M. Thus, there are at most $2\Delta - 2$ forbidden colors for the edge (u, v) in total. So there is at least one available color to color u and v. ◀

▶ **Theorem 11.** *Let $k \in \mathbb{N}^*$. Let $\mathcal{C}$ be a class of graphs such that, for every $G \in \mathcal{C}$, if G has a perfect matching then G has a k-matching coloring. Then, in the anonymous model at*

distance 1, k certificates are enough to certify the existence of a perfect matching in G for every $G \in \mathcal{C}$.

Proof of Theorem 11. Let $G = (V, E)$ be a graph in $\mathcal{C}$ having a perfect matching. Let φ be a k-matching coloring of G. For every v, the prover gives the certificate $c(v) := \varphi(v)$ to the vertex v.

For every $G \in \mathcal{C}$ and certificate function c, every vertex v checks the certificate as follows: v checks if it has exactly one neighbor u such that $c(u) = c(v)$. If it is the case, v accepts. Otherwise, v rejects.

It remains to show that a graph $G \in \mathcal{C}$ is accepted if and only if it has a perfect matching. If G has a perfect matching, then every vertex accepts with the certificate function given by the prover described above, by definition of a matching coloring. Conversely, if all the vertices accept, we construct a perfect matching by matching each vertex v to the unique vertex u in his neighborhood such that $c(u) = c(v)$. ◀

Lemma 28 and Theorem 11 directly implies that the following holds:

▶ **Corollary 12.** *For every graph G, $2\Delta - 1$ certificates are enough to certify the existence of a perfect matching, in the anonymous model at distance 1.*

We will see in Section 6.2 that the dependency on Δ is unavoidable in the anonymous model, and unavoidable in the locally checkable proofs model when verification algorithms consist in checking for a matching coloring.

One can wonder if the dependency on Δ is always unavoidable, or if there exist some non-trivial graph classes with a certification of constant size. We give a very short proof that such graph classes exist, *e.g.* planar graphs:

▶ **Theorem 29.** *Let $k \in \mathbb{N}$. Let $\mathcal{C}$ be a class of graphs closed by edge contraction such that for all $G \in \mathcal{G}$, the chromatic number of G is at most k. Then, k certificates are enough to certify a perfect matching for graphs in $\mathcal{C}$.*

Proof. By Theorem 11, it is sufficient to show that for every $G \in \mathcal{C}$, if G has a perfect matching then G has a k-matching coloring.

Let $G \in \mathcal{C}$ such that G has a perfect matching M. Let us define a k-matching coloring φ of G. Let G' be the graph obtained from G by contracting every edge of M. Since $\mathcal{C}$ is closed by edge contraction, $G' \in \mathcal{C}$ so G' also is k-colorable. Let φ' be a proper k-coloring of G'. For every vertex $u \in V(G)$, there exists a unique edge $e \in M$ such that $u \in e$. Let $u' \in V(G')$ be the vertex of G' resulting from the contraction of e. Let $\varphi(u) := \varphi'(u')$. Then, φ is a k-matching coloring of G (because M is a perfect matching and φ' is a proper k-coloring of G'). ◀

The following corollary is a direct consequence of Theorem 29 and classical theorems of structural graph theory.

▶ **Corollary 13.** *In the anonymous model at distance 1:*

- *Only 2 bits are enough to certify the existence of a perfect matching for planar graphs.*
- *Only $O(\log k)$ bits are needed to certify the existence of a perfect matching in K_k-minor-free graphs.*
- *Only $\lceil \log_2(k+1) \rceil$ bits are needed to certify the existence of a perfect matching in graphs of treewidth at most k.*

Proof. The first statement is a consequence of the 4-color theorem. The second point follows from the best bound known on Hadwiger's conjecture by Delcourt and Postle [10]. The last statement simply follows from the fact that edge contractions cannot increase the treewidth and graphs of treewidth k are k-degenerate (and then $(k+1)$-colorable). ◀

Note that the behavior on planar graphs is completely different in the three properties we considered: for coloring, we get a tight bound of 4 certificates, for dominating sets at distance t, the general lower bounds hold, and for certification of perfect matchings, the natural approach which gives $O(\Delta)$ certificates can be drastically improved.

6.2 Lower bounds

The first result of this section consists in proving that the number of bits obtained in Corollary 12 to certify that a graph admits a perfect matching is (essentially) tight.

▶ **Theorem 14.** *For every $\Delta \geqslant 2$, in the anonymous model where vertices can see at distance 1, Δ different certificates are needed to certify the existence of a perfect matching for graphs of maximum degree Δ.*

Proof. Assume by contradiction that $\Delta - 1$ certificates are sufficient to certify the existence of a perfect matching for graphs with maximum degree at most Δ.

Let $B_\Delta = (V_\Delta, E_\Delta)$ be the bipartite graph on vertex set $V_\Delta := \{u_1, \dots, u_\Delta\} \cup \{v_1, \dots, v_\Delta\}$, and (u_i, v_j) is an edge for every $i \geqslant j$. This graph is usually called a *half graph*. The graph B_Δ has a perfect matching (consisting of the edges (u_i, v_i) for all $i \in \{1, \dots, \Delta\}$). Thus, there exists a certificate function $c : V_\Delta \to \{1, \dots, \Delta - 1\}$ which makes every vertex accept. It is easy to check that there actually is a unique perfect matching in B_Δ. By pigeonhole principle, there must exist $1 \leqslant j_1 < j_2 \leqslant \Delta$ such that $c(v_{j_1}) = c(v_{j_2})$. See Figure 5 for illustration.

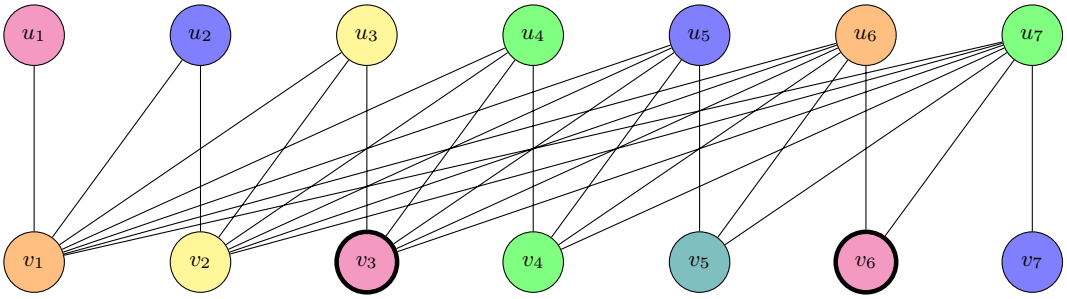

Figure 5 The graph B_7 with an accepting certificate assignment (that we will use in the next pictures). Here, certificates are represented by the colors, and only 6 different certificates are used. In this example, we take $j_1 = 3$ and $j_2 = 6$.

To obtain a contradiction, we construct a graph G_Δ which does not have a perfect matching, but has a certificate function such that all the vertices accept. We construct G_Δ as follows. We take two copies of B_Δ, denoted by B'_Δ and B''_Δ. We denote by $V'_\Delta = \{u'_1, v'_1, \dots\}$ (resp. $V''_\Delta = \{u''_1, v''_1, \dots\}$) the vertex set of B'_Δ (resp. B''_Δ). For all $i \in \{j_1, \dots, j_2 - 1\}$, we delete the edge (u''_i, v''_{j_1}) and we add the edge (u''_i, v'_{j_2}). Finally, the prover gives to the vertices of B'_Δ and B''_Δ their certificates in B_Δ. For instance, with the certificates of B_7 represented in Figure 5, the graph G_7 receives the certificates represented in Figure 6.

▷ Claim 30. The graph G_Δ does not have a perfect matching.

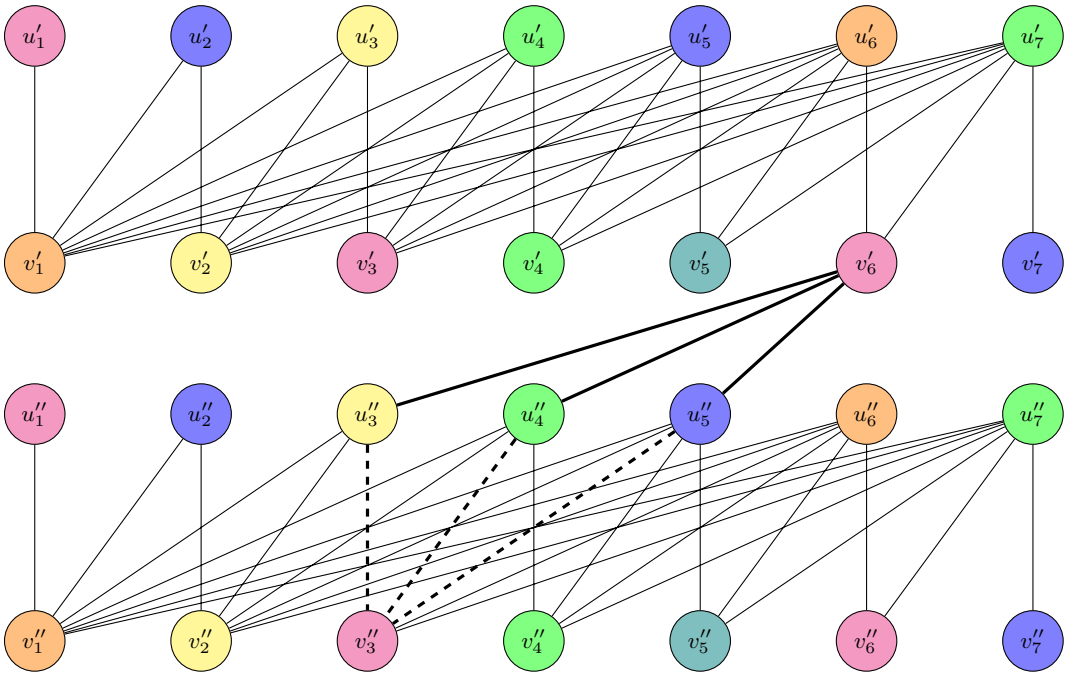

Figure 6 The graph G_7, with the certificates used in the proofs. Dashed edges represent edges that have been removed when building G_7. The sets used in Claim 30 are $A = \{v''_3, v''_6, v''_7\}$ and $N(A) = \{u''_6, u''_7\}$.

Proof. The set $A = \{v''_{j_1}, v''_{j_2}, v''_{j_2+1}, \ldots, v''_\Delta\}$ is an independent set of size $\Delta - j_2 + 2$. And $N(A)$ is $\{u''_{j_2}, \ldots, u''_\Delta\}$, which is a set of size $\Delta - j_2 + 1$. Therefore, not all vertices of A can be matched. ◀

We show that the certificates given by the prover as described previously make all vertices of G_Δ accept. In the graph G_Δ, all the vertices of B'_Δ have the same view as their copy in B_Δ, except v'_{j_2} which has the view of v_{j_1} in B_Δ. Since all the vertices of B_Δ accept, all the vertices of B'_Δ accept as well. Similarly, in B''_Δ, all the vertices have the same view as their copy in B_Δ, except v''_{j_1} which has the view of v_{j_2} in B_Δ. Note that, for $u''_{j_1}, \ldots, u''_{j_2-1}$, it is because $c(v_{j_1}) = c(v_{j_2})$. Thus, all the vertices of B''_Δ accept. So all the vertices of G_Δ accept. Together with Claim 30, this is a contradiction. ◀

We can now wonder if fewer certificates are needed in the locally checkable proofs model. We did not succeed to answer this question in full generality, but we prove the result for a specific type of certification. Remember that in the proof of Theorem 11 with the matching coloring, the vertices check independently their neighbors in order to look for an edge of the matching. Every vertex then accepts if it is adjacent to exactly one edge of the matching. In other words, by looking only at the certificates and identifiers of its endpoints, each edge can be described as *valid* or *invalid*, in the sense that the nodes consider it to be an edge of the matching or not. Each vertex accepts if and only if it is the endpoint of exactly one valid edge. We call such a checking algorithm a *constructive* checking. If we have a constructive checking which makes every vertex accept, it is possible to construct a perfect matching simply by matching each vertex with the endpoint of its valid edge. Note that, as in the proof of Theorem 11, $2\Delta - 1$ different certificates are always sufficient to certify a perfect

matching with a constructive checking. In fact, we will show that it is optimal (up to a constant factor on the number of bits).

▶ **Theorem 31.** *In the locally checkable proofs model, for every $\Delta \geqslant 1$, at least $\Omega(\log \Delta)$ bits are needed to certify a perfect matching with a constructive checking.*

Proof. Assume that m bits are sufficient to certify a perfect matching with a constructive checking. Let us fix 2Δ different identifiers, denoted by $Id_1, \ldots, Id_{2\Delta}$. Let us consider the bipartite graph $B_\Delta = (V_\Delta, E_\Delta)$ introduced in the proof of Theorem 14. For each permutation σ of $\{1, \ldots, \Delta\}$, let us consider $B_\Delta(\sigma)$ the graph where each vertex u_i has the identifier $Id_{\sigma(i)}$, and each vertex v_i the identifier $Id_{\Delta+i}$. Since $B_\Delta(\sigma)$ has a perfect matching, there exists a certificate function $c_\sigma : \{Id_1, \ldots, Id_{2\Delta}\} \to \{0, \ldots, 2^m - 1\}$ which makes all vertices of $B_\Delta(\sigma)$ accept.

▷ Claim 32. Let σ, τ be two permutations of $\{1, \ldots, \Delta\}$ such that $c_\sigma = c_\tau$. Then, $\sigma = \tau$.

Proof of Claim 32. Let σ, τ be such that $c_\sigma = c_\tau$. By definition of a constructive verification, the set of valid edges in the graph $B_\Delta(\sigma)$ certified with c_σ is a perfect matching. Since the only perfect matching in B_Δ is $\{(u_1, v_1), \ldots, (u_\Delta, v_\Delta)\}$, it is the set of valid edges in $B_\Delta(\sigma)$ certified with c_σ.

By contradiction, assume that $\sigma \neq \tau$. Let i_0 the smallest element of $\{1, \ldots, \Delta\}$ such that $\sigma(i_0) \neq \tau(i_0)$. In $B_\Delta(\tau)$, the edge (u_{i_0}, v_{i_0}) is valid (because valid edges form a perfect matching). Let j_0 be such that vertex $\tau(j_0) = \sigma(i_0)$. By definition of i_0, we get $j_0 \in \{i_0 + 1, \ldots, \Delta\}$. Since $c_\sigma = c_\tau$, the edge (u_{j_0}, v_{i_0}) has same identifiers and certificates than edge (u_{i_0}, v_{i_0}) in $B_\Delta(\sigma)$. Thus, the edge (u_{j_0}, v_{i_0}) is also valid in $B_\Delta(\tau)$. This is a contradiction because vertex v_{i_0} would then be the endpoint of two valid edges in $B_\Delta(\tau)$, so it should reject. ◀

We can now conclude the proof of Theorem 31. Assume that m bits are sufficient to certify a perfect matching in the locally checkable proofs model, with a constructive verification algorithm. By Claim 32, the number of different functions $\{Id_1, \ldots, Id_{2\Delta}\} \to \{0, \ldots, 2^m - 1\}$ is at least the number of permutations of $\{1, \ldots, \Delta\}$. Thus, we get $2^{2m\Delta} \geqslant \Delta!$, leading to $m \geqslant \frac{\log_2(\Delta!)}{2\Delta}$. Since $\log_2(\Delta!) = \Omega(\Delta \log \Delta)$, we get the result. ◀

References

1. Alkida Balliu, Sebastian Brandt, Juho Hirvonen, Dennis Olivetti, Mikaël Rabie, and Jukka Suomela. Lower bounds for maximal matchings and maximal independent sets. *J. ACM*, 68(5):39:1–39:30, 2021.
2. Samuel Bernard, Stéphane Devismes, Maria Gradinariu Potop-Butucaru, and Sébastien Tixeuil. Optimal deterministic self-stabilizing vertex coloring in unidirectional anonymous networks. In *23rd IEEE International Symposium on Parallel and Distributed Processing, IPDPS 2009*, pages 1–8, 2009.
3. Aviv Bick, Gillat Kol, and Rotem Oshman. Distributed zero-knowledge proofs over networks. In *Proceedings of the 2022 ACM-SIAM Symposium on Discrete Algorithms, SODA 2022*, pages 2426–2458. SIAM, 2022.
4. Nicolas Bousquet, Laurent Feuilloley, and Théo Pierron. What can be certified compactly? compact local certification of MSO properties in tree-like graphs. In *PODC '22: ACM Symposium on Principles of Distributed Computing*, pages 131–140, 2022.
5. Sebastian Brandt and Dennis Olivetti. Truly tight-in-Δ bounds for bipartite maximal matching and variants. In *PODC '20: ACM Symposium on Principles of Distributed Computing*, pages 69–78, 2020.

6 Jesper Makholm Byskov. Enumerating maximal independent sets with applications to graph colouring. *Oper. Res. Lett.*, 32(6):547–556, 2004.

7 Keren Censor-Hillel, Ami Paz, and Mor Perry. Approximate proof-labeling schemes. *Theor. Comput. Sci.*, 811:112–124, 2020.

8 Johanne Cohen, Jonas Lefèvre, Khaled Maâmra, Laurence Pilard, and Devan Sohier. A self-stabilizing algorithm for maximal matching in anonymous networks. *Parallel Process. Lett.*, 26(4):1650016:1–1650016:17, 2016.

9 Amin Coja-Oghlan, Charilaos Efthymiou, and Samuel Hetterich. On the chromatic number of random regular graphs. *J. Comb. Theory, Ser. B*, 116:367–439, 2016.

10 Michelle Delcourt and Luke Postle. Reducing linear hadwiger's conjecture to coloring small graphs. *CoRR*, abs/2108.01633, 2021.

11 Yuval Emek and Yuval Gil. Twenty-two new approximate proof labeling schemes. In *34th International Symposium on Distributed Computing, DISC 2020*, volume 179, pages 20:1–20:14, 2020.

12 P Erdős and A Rényi. On the existence of a factor of degree one of a connected random graph. *Acta Mathematica Hungarica*, 17(3-4):359–368, 1966.

13 Paul Erdös. Graph theory and probability. *Canadian Journal of Mathematics*, 11:34–38, 1959.

14 Laurent Feuilloley. Introduction to local certification. *Discret. Math. Theor. Comput. Sci.*, 23(3), 2021.

15 Laurent Feuilloley, Pierre Fraigniaud, Juho Hirvonen, Ami Paz, and Mor Perry. Redundancy in distributed proofs. *Distributed Comput.*, 34(2):113–132, 2021.

16 Michael J. Fischer and Hong Jiang. Self-stabilizing leader election in networks of finite-state anonymous agents. In Alexander A. Shvartsman, editor, *Principles of Distributed Systems, 10th International Conference, OPODIS 2006*, volume 4305, pages 395–409, 2006.

17 Orr Fischer, Rotem Oshman, and Dana Shamir. Explicit space-time tradeoffs for proof labeling schemes in graphs with small separators. In *25th International Conference on Principles of Distributed Systems, OPODIS 2021*, volume 217 of *LIPIcs*, pages 21:1–21:22, 2021.

18 Pierre Fraigniaud, Frédéric Mazoit, Pedro Montealegre, Ivan Rapaport, and Ioan Todinca. Distributed certification for classes of dense graphs. *CoRR*, abs/2307.14292, 2023.

19 Pierre Fraigniaud, Pedro Montealegre, Ivan Rapaport, and Ioan Todinca. A meta-theorem for distributed certification. In *Structural Information and Communication Complexity - 29th International Colloquium, SIROCCO 2022*, volume 13298, pages 116–134, 2022.

20 Mika Göös and Jukka Suomela. Locally checkable proofs in distributed computing. *Theory Comput.*, 12(1):1–33, 2016.

21 Amos Korman, Shay Kutten, and David Peleg. Proof labeling schemes. *Distributed Comput.*, 22(4):215–233, 2010.

22 Virgina Ardévol Martínez, Marco Caoduro, Laurent Feuilloley, Jonathan Narboni, Pegah Pournajafi, and Jean-Florent Raymond. Lower bound for constant-size local certification. In *Stabilization, Safety, and Security of Distributed Systems - 24th International Symposium, SSS 2022*, volume 13751, pages 239–253, 2022.

23 Moshe Morgenstern. Existence and explicit constructions of $q + 1$ regular ramanujan graphs for every prime power q. *J. Comb. Theory, Ser. B*, 62(1):44–62, 1994.

24 Rafail Ostrovsky, Mor Perry, and Will Rosenbaum. Space-time tradeoffs for distributed verification. In *Structural Information and Communication Complexity - 24th International Colloquium, SIROCCO 2017*, volume 10641, pages 53–70, 2017.

25 Jukka Suomela. Using round elimination to understand locality. *SIGACT News*, 51(3):63–81, 2020.

26 Nicolas Trotignon. Perfect graphs: a survey. *CoRR*, abs/1301.5149, 2013.

27 Jonathan S. Turner. Almost all k-colorable graphs are easy to color. *J. Algorithms*, 9(1):63–82, 1988.