What can be certified compactly?
Compact local certification of MSO properties in tree-like graphs

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
Théo Pierron — Univ Lyon, UCBL, CNRS, INSA Lyon, LIRIS, UMR5205, F-69622 Villeurbanne, France

Abstract

Local certification consists in assigning labels (called *certificates*) to the vertices of a graph G, in order to certify a property of G. The verification of this certification must be local: a node typically sees only its neighbors. The main measure of performance of a certification is the size of its certificates, which can be seen as a measure of the globality of the property.

A certification with labels of size $O(\log n)$ is called *compact*. It is known that being planar, having bounded-genus, and forbidding some minors are properties that have compact certifications.

In this work, we are interested in meta-theorems (similar to Courcelle's theorem). We design compact certification for MSO logic on trees and bounded-treedepth graphs, and prove matching lower bounds. (Full version: arxiv:2202.06065.)

1 Introduction

1.1 Local certification

In this work, we are interested in the locality of graph properties. For example, consider the property "the graph has maximum degree three". We say that this property can be checked locally, because if every node checks that it has at most three neighbors (which is a local verification), then the graph satisfies the property (which is a global statement). Most graph properties of interest are not local. For example, to decide whether a graph is acyclic, or planar, the vertices would have to look arbitrarily far in the graph.

The notion of local certification originates from distributed computing, where local detection of faults is essential. It is a labeling-mechanism allowing any graph property to be checked locally. For a given property, a local certification is described by a certificate assignment and a verification algorithm: each node receives a certificate, reads the certificates of its neighbors and then runs a verification algorithm. This algorithm decides whether the node accepts or rejects the certification. If the graph satisfies the property, then there should be a certificate assignment such that all the nodes accept. Otherwise, in each assignment, there must be at least one node that rejects.

1.2 Understanding the power of compact local certification

It is known that any property can be certified with $O(n^2)$ bits certificates, where n is the total number of vertices. This is because one can simply give the full description of the graph to every node, which can then check that the property holds in the graph described, and that the graph description is correct locally, and identical between neighbors. This $O(n^2)$ size is extremely large, and the main goal of the study of local certification is to minimize the size of the certificate, expressed as a number of bits per vertex, as a function of n. In addition to the optimization motivation originating from distributed self-stabilizing algorithms, establishing the minimum certificate size also has a more theoretical appeal. Indeed, the optimal certification size of a property can be seen as a measure of its locality: the smaller the labels, the less global information we need to allow local verification, the more local the property.

Over the years, it was identified that $\Theta(\log n)$ was a special certificate size. Indeed, on the one hand, for most properties, one cannot hope to go below this size per node. For example, certifying acyclicity requires $\Omega(\log n)$ [10]. On the other hand, once we have a logarithmic number of bits, we can encode identifiers, and distances, which is enough for spanning trees, an essential tool in certification. A certification with $\Theta(\log n)$ bits is now called a *compact local certification*, and it has become the gold standard of the area. Recently, planarity and more generally embeddability on bounded-genus surfaces, and H-minor-freeness for graphs H of size at most 4, have been proved to have such compact certifications [8, 6, 1].

Unfortunately, not every property has a compact certification. For example, having a non-trivial automorphism or not being 3-colorable are properties that cannot be certified with less than $\Omega(n^2)$ bits [10]. Even surprisingly simple properties, such as having diameter at most 2, cannot be certified with a sublinear number of bits per vertex (up to logarithmic factors), if we only allow the local verification to be at distance one [2]. This raises the following question:

Question: What are the graph properties that admit a compact local certification?

2 Our approach, results, and techniques

2.1 A systematic model checking approach

As mentioned above, many specific graph properties such as planarity or small-diameter have been studied in the context of local certification. In this paper, we are interested in establishing theorems of the form: "all the properties that can be expressed in some formalism X have a compact certification". We will consider properties that can be expressed by sentences from monadic second order logic (MSO), just like in Courcelle's theorem. These are formed from atomic predicates that test equality or adjacency of vertices and allowing boolean operations and quantifications on vertices, edges, and sets of vertices or edges.

2.2 The generic case

Let us first discuss what such a meta-theorem must look like when we do not restrict the class of graphs we consider. As we already mentioned, graphs of diameter at most 2 cannot be certified with sublinear certificates [2]. This can be expressed with the following sentence:

$$\forall x \forall y (x = y \vee x - y \vee \exists z (x - z \wedge z - y))$$

This sentence is very simple: it is a first order sentence (a special case of MSO), it has quantifier depth three and there is only one quantifier alternation (two standard complexity measures for FO sentences which respectively counts the maximum number of nested quantifiers and the number of alternations between blocks of existential and universal quantifiers). Therefore, there exists very simple first order logic sentences which cannot be certified efficiently, hence there is no room for a generic $O(\log n)$ result.

2.3 The case of trees

The classic approach in centralized computing is then to restrict the class of the graphs considered. This is also relevant here: for example, certifying some given diameter is easier if we restrict the graphs to trees. Indeed, in this case we can use a spanning tree to point to a central vertex (or edge), that becomes a root (or root-edge), and keep at every vertex both its distance to the root and the depth of its subtree. This certification can be checked by simple distance comparisons, and it uses $O(\log n)$ bits. The first of our main results is that we can actually get a better bound (constant certificates) for all MSO properties on trees, via the simulation of a tree automata.

Theorem 1. *Any MSO formula can be certified on trees with certificates of size* $O(1)$*.*

One can wonder if we can extend this statement to a significantly wider logic. We answer by the negative by proving that some typical non-MSO properties cannot be certified with certificates of sublinear sizes even on trees of bounded depth.

Theorem 2. *Certifying the trees that have an automorphism without fixed-point requires certificates of size* $\tilde{\Omega}(n)$ *(where* $\tilde{\Omega}$ *hides polylogarithmic factors), even if we restrict to trees of bounded depth.*

2.4 The case of bounded treedepth graphs

In centralized model checking, a classic meta-theorem of Courcelle [3] establishes that all the problems expressible in MSO can be solved in polynomial-time in graphs of bounded treewidth. One can wonder if some Courcelle-like result holds for certification. Namely, is it possible to certify any MSO-formula on graphs of bounded treewidth with certificates of size $O(\log n)$? Prior to our work, it was not known whether graphs of fixed width can be certified with logarithmic size certificates. Proving such a statement is a preliminary condition for MSO-certification, since certifying a property on a graph class we cannot certify may lead to aberrations.

We prove that one can locally check that a graph has treedepth at most t with logarithmic-size certificates.

Theorem 3. *We can certify that a graph has treedepth at most* t *with* $O(t \log n)$ *bits.*

We also show that Theorem 3 is optimal, in the sense that certifying treedepth at most k requires $\Omega(\log n)$ bits, even for small k.

Theorem 4. *Certifying that the treedepth of the graph is at most* k *requires* $\Omega(\log n)$ *bits, for any* $k \geq 5$*.*

The proof technique here is a reduction from communication complexity. Note that this result contrasts with the fact that certifying trees of depth k can be done with $O(\log k)$ bits (thus independent of n), by simply encoding distances to the root.

The next problem in line is then MSO-model checking for graphs of bounded treedepth. In such classes, it happens that MSO and FO have the same expressive power [4]: for every t and every MSO sentence, there exists a FO sentence satisfied by the same graphs of treedepth at most t.

Theorem 5. *Every FO (and hence MSO) sentence* φ *can be locally certified with* $O(t \log n + f(t, \varphi))$*-bit certificates on graphs of treedepth at most* t*.*

The core of the proof here is a locally certifiable kernelization of bounded-treedepth graphs for MSO properties.

Inspired by our results and techniques, Fraigniaud, Montealegre, Rapaport, and Todinca, very recently proved that it is possible to certify MSO properties in bounded treewidth graphs, with certificates of size $\Theta(\log^2 n)$ [9]. It is a fascinating question whether this is optimal or can be reduced down to $O(\log n)$.

Theorem 5 has an interesting corollary for the certification of graphs with forbidden minors. An important open question in the field of local certification is to establish whether all the graph classes defined by a set of forbidden minors have a compact certification. Note that this question generalizes the results about planarity and bounded-genus graphs of [8, 6]. Very recently, Bousquet, Feuilloley and Pierron proved that the answer is positive for all minors of size at most 4 [1], but the question is still wide open for general minors. Theorem 5 leads to the following result, where P_t and C_t are respectively the path and the cycle of length t.

Corollary 1. *For all t, P_t-minor-free graphs and C_t-minor-free graphs can be certified with $O(\log n)$-bit certificates.*

Still related to the certification of minors, Esperet and Norin [7] (generalizing a result by Elek [5]) proved very recently that certifying that a graph belongs to a minor-closed class or is far from it (in the sense of the edit distance, as in property testing) can be done with constant size certificate. Using our certification of bounded treedepth, they generalize this result to all monotone properties of minor-closed classes, with $O(\log n)$-size certificates.

References

[1] Nicolas Bousquet, Laurent Feuilloley, and Théo Pierron. Local certification of graph decompositions and applications to minor-free classes. In *25th International Conference on Principles of Distributed Systems, OPODIS 2021*, volume 217 of *LIPIcs*, pages 22:1–22:17, 2021.

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

[3] Bruno Courcelle. The monadic second-order logic of graphs. i. recognizable sets of finite graphs. *Inf. Comput.*, 85(1):12–75, 1990.

[4] Michael Elberfeld, Martin Grohe, and Till Tantau. Where first-order and monadic second-order logic coincide. *ACM Trans. Comput. Log.*, 17(4):25:1–25:18, 2016.

[5] Gábor Elek. Planarity is (almost) locally checkable in constant-time. *CoRR*, abs/2006.11869, 2020.

[6] Louis Esperet and Benjamin Lévêque. Local certification of graphs on surfaces. *Theor. Comput. Sci.*, 2022.

[7] Louis Esperet and Sergey Norin. Testability and local certification of monotone properties in minor-closed classes. *CoRR*, abs/2202.00543, 2022

[8] Laurent Feuilloley, Pierre Fraigniaud, Pedro Montealegre, Ivan Rapaport, Éric Rémila, and Ioan Todinca. Compact distributed certification of planar graphs. *Algorithmica*, 83(7):2215–2244, 2021.

[9] Pierre Fraigniaud, Pedro Montealegre, Ivan Rapaport, and Ioan Todinca. A meta-theorem for distributed certification. *CoRR*, abs/2112.03195, 2021.

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