What can be certified compactly?

Compact local certification of MSO properties in tree-like graphs

Nicolas Bousquet, Laurent Feuilloley, Théo Pierron

University of Lyon 1 and CNRS

ICGT, Montpellier, July 2022
What can be certified compactly?

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

Compact local certification of MSO properties in tree-like graphs

Unofficial subsubtitle:
Distributed computing on graphs
meets model checking
meets parameterized complexity
What can be certified compactly?

Compact local certification of MSO properties in tree-like graphs

Unofficial subsubtitle:
Distributed computing on graphs
  *meets* model checking
  *meets* parameterized complexity

Disclaimer: citations are at the end, send me emails if you want pointers.
Distributed computing motivation

A model of distributed computing:

- Network represented by a graph.
- Computation step: a vertex accesses the state of its neighbors and updates its state.
Distributed computing motivation

A model of distributed computing:
- Network represented by a graph.
- Computation step: a vertex accesses the state of its neighbors and updates its state.
Distributed computing motivation

A model of distributed computing:

- Network represented by a graph.
- Computation step: a vertex accesses the state of its neighbors and updates its state.

- There are faults: some set of states can be modified arbitrarily.
- Goal: converge to a correct solution (e.g., a spanning tree).
Distributed computing motivation

A simpler problem: Check correctness. If not correct: a node should raise an alarm.

Examples: 3-coloring and spanning tree
Distributed computing motivation

A simpler problem: Check correctness. If not correct: a node should raise an alarm.

Examples: 3-coloring and spanning tree
Distributed computing motivation

A simpler problem: Check correctness. If not correct: a node should raise an alarm.

Examples: 3-coloring and spanning tree
Distributed computing motivation

A simpler problem: Check correctness. If not correct: a node should raise an alarm.

Examples: 3-coloring and spanning tree
Distributed computing motivation

A simpler problem: Check correctness. If not correct: a node should raise an alarm.

Examples: 3-coloring and spanning tree

Problem: Acyclicity is a global property that cannot be checked locally.
Distributed computing motivation

A simpler problem: Check correctness.
If not correct: a node should raise an alarm.

Examples: 3-coloring and spanning tree

Problem: Acyclicity is a global property that cannot be checked locally.
Solution: Keep additional information to certify the correctness.
Moving towards graphs

Now: checking that the graph belongs to a given class.

Let \( C \) be a class of connected graphs.

**A local decision algorithm:** a mapping from the neighborhoods at distance \( d \) \( (d = 1 \) here) to *accept* or *reject*.

**Local recognition of \( C \):** A local decision algorithm such that:

- If \( G \in C \) then all the vertices accept.
- If \( G \notin C \) then at least one vertex rejects.

**Doable:** Locally recognize cycles. (Check degree=2)

**Not doable:** Locally recognize paths.
Local certification (intuition)

$\mathcal{C} = \text{trees}$

Imagine the graph comes with labels, that are supposed to be the distances to a root.
Local certification (intuition)

\[ \mathcal{C} = \text{trees} \]

Imagine the graph comes with labels, that are supposed to be the distances to a root.

A local decision algorithm: accept iff the distances are consistent.
Local certification (intuition)

$C = \text{trees}$

Imagine the graph comes with labels, that are supposed to be the distances to a root.

A local decision algorithm: accept iff the distances are consistent.

Fact: there exists a labeling that is consistent everywhere iff the graph is a tree.
Local certification (definition)

A local certification (of size \(k\)) for a class \(C\) is a local decision algorithm such that:

1. For \(G \in C\), there exists certificate assignment (of \(k\)-bit labels) that makes all vertices accept.
2. For \(G \notin C\), for any certificate assignment (of \(k\)-bit labels), at least one vertex rejects.

Several points of view on the notion:

- Fault-tolerance, self-stabilization.
- A distributed analogue of NP.
- Extension to the space of labeled graphs s.t.: the checking is local in this space, and the projection to unlabeled is \(C\).
Can we certify any graph class?

Question: Take a graph class $\mathcal{C}$ (i.e. an infinite set of graphs). Does there exists a local certification?

Answer: Yes (with the help of identifiers). Size: $\Theta(n^2)$. 
Optimal certificate size

Measure of quality: the size of the certificates.

Example: for trees,

- the optimal certificate size for trees is $\geq 1$, and $\leq O(n^2)$,
- the distance labeling gives $O(\log n)$
- $O(\log n)$ is actually optimal

$\rightarrow$ The (optimal) certificate size is a measure of locality.
Landscape of certificate sizes

Compact certification = $O(\log n)$ certificates (or polylog($n$)):

- $k$-colorable graphs: $O(\log k)$
- paths, trees: $\Theta(\log n)$
- planar, bounded-genus: $\Theta(\log n)$

Terribly non-compact certification:

- diameter $\leq 3$: $\tilde{\Theta}(n)$
- non $k$-colorable: $\tilde{\Theta}(n^2)$
- symmetric graphs: $\Theta(n^2)$ (and $\tilde{\Theta}(n^2)$ for symmetric trees.)

Intriguing open question: Does every minor-closed class admit a compact certification?
Landscape of certificate sizes

Compact certification = $O(\log n)$ certificates (or polylog($n$)):

- $k$-colorable graphs: $O(\log k)$
- paths, trees: $\Theta(\log n)$
- planar, bounded-genus: $\Theta(\log n)$

Terribly non-compact certification:

- diameter $\leq 3$: $\tilde{\Theta}(n)$
- non $k$-colorable: $\tilde{\Theta}(n^2)$
- symmetric graphs: $\Theta(n^2)$ (and $\tilde{\Theta}(n)$ for symmetric trees.)
Landscape of certificate sizes

Compact certification = $O(\log n)$ certificates (or polylog($n$)):

- $k$-colorable graphs: $O(\log k)$
- paths, trees: $\Theta(\log n)$
- planar, bounded-genus: $\Theta(\log n)$

Terribly non-compact certification:

- diameter $\leq 3$: $\tilde{\Theta}(n)$
- non $k$-colorable: $\tilde{\Theta}(n^2)$
- symmetric graphs: $\Theta(n^2)$ (and $\tilde{\Theta}(n)$ for symmetric trees.)

Intriguing open question: Does every minor-closed class admit a compact certification?
What about meta-theorems?

Courcelle’s theorem: Any MSO property can be decided in linear time when the treewidth of the graph is bounded.

MSO properties: Logical formula built with:
\((u, v) \in E, \exists u, \forall u, \exists S \subset V, \forall S \subset V\), and usual connectors.
What about meta-theorems?

Courcelle’s theorem: Any MSO property can be decided in linear time when the treewidth of the graph is bounded.

MSO properties: Logical formula built with:

\[(u, v) \in E, \exists u, \forall u, \exists S \subset V, \forall S \subset V,\] and usual connectors.

Theorem we are looking for: Any property XXX can be certified with \(O(\log n)\) labels, when the YYY of the graph is bounded.

Note: restricting both the logic and the structure is also necessary for compact certification:

- Diameter \(> 3\) is in \(FO\), but certificate size is \(\tilde{\Omega}(n)\)
- Symmetric trees are... trees, but certificate size is \(\tilde{\Omega}(n)\)
On trees

**Theorem**: Any MSO property can be certified with $O(1)$ bits in trees.

**Technique on edge-labeled oriented paths (≡ words)**:

- Known theorem: MSO on path = regular languages
- Use the automaton states as labels.
On bounded-tree-depth

**Theorem**: Any MSO property can be certified with $O(\log n)$ bits in graphs of bounded treedepth.
On bounded-treedepth

**Theorem**: Any MSO property can be certified with $O(\log n)$ bits in graphs of bounded treedepth.
On bounded-treedepth

**Theorem:** Any MSO property can be certified with $O(\log n)$ bits in graphs of bounded treedepth.
On bounded-treeldepth

**Theorem**: Any MSO property can be certified with $O(\log n)$ bits in graphs of bounded treedepth.
Other results and open questions

- An analogue for treewidth has been proved with certificates of size $O(\log^2 n)$ bits. Is it optimal?
- Other trade-offs between expressivity/structure/certification?
- Certifying all minor-closed classes in $O(\log n)$?
- What about completely different type of classes, like unit-disks?
Bibliographic pointers

Local certification papers mentioned:

- Proof-labeling schemes (Korman, Kutten, Peleg - 2010). doi:10.1007/s00446-010-0095-3
- Locally checkable proofs in distributed computing (Göös, Suomela - 2016). doi:10.4086/toc.2016.v012a019

Tutorial on local certification

Certification of planar and bounded-genus graphs

- Compact distributed certification of planar graphs (Feuilloley, Fraigniaud, Montealegre, Rapaport, Rémila, Todonca, 2021) doi:10.1007/s00453-021-00823-w + Talks at PODC by Montealegre
- Local Certification of Graphs with Bounded Genus (Same as above.) arxiv:2007.08084
- Local certification of graphs on surfaces (Esperet, Leveque - 2021) arxiv:2102.04133

Small diameter lower bound

Bibliographic pointers

Certification of $H$-minor-free graphs

- Local certification of graph decompositions and applications to minor-free classes (Bousquet, Feuilloley, Pierron - 2021) arxiv:2108.00059 + BA at DISC.

Other specific classes

- Compact Distributed Interactive Proofs for the Recognition of Cographs and Distance-Hereditary Graphs (Montealegre, Ramírez-Romero, and Rapaport - 2021) arxiv:2012.03185 (+ personal communication)

MSO on bounded treewidth

- A Meta-Theorem for Distributed Certification (Fraigniaud, Montealegre, Rapaport, Ioan Todinca - 2022)