What can be certified compactly?

Compact local certification of MSO properties in tree-like graphs

Nicolas Bousquet, Laurent Feuilloley, Théo Pierron

CNRS and University of Lyon 1

PODC 2022, Salerno

Disclaimer: almost no citations in the slides, bibliography at the end.

Introduction to local certification

Idea: A local certification is some information stored at the nodes of a network to allow quick checking of correctness.

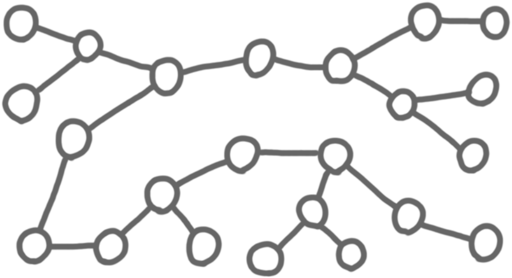
Abstraction: A labeling of the vertices of a graph to allow local decision of a property.

Origin: A general framework for self-stabilization: if the quick checking of the current configuration fails, do something to fix it.

Nowadays: Studied on its own, both for checking data structures (*e.g.* spanning trees), and networks properties (*e.g.* planarity).

Example and definition

Example: Checking acyclicity.

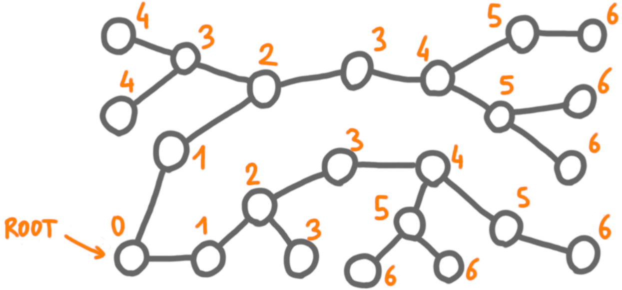


Example and definition

Example: Checking acyclicity.

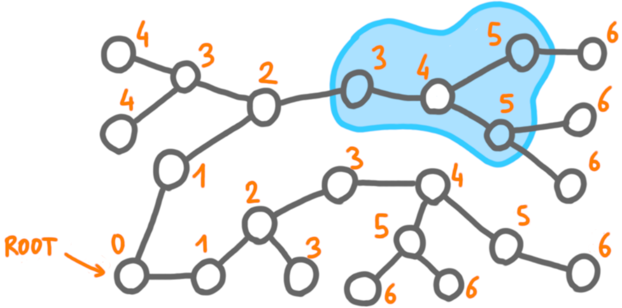
Example and definition

Example: Checking acyclicity.



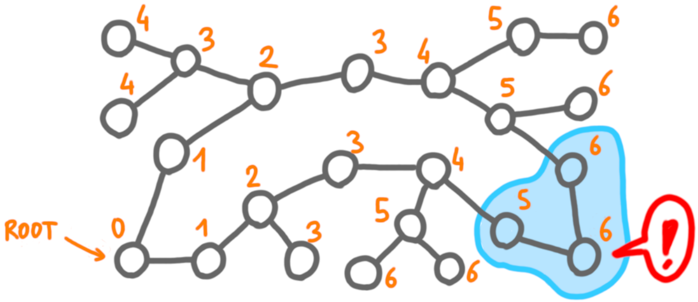
Example and definition

Example: Checking acyclicity.



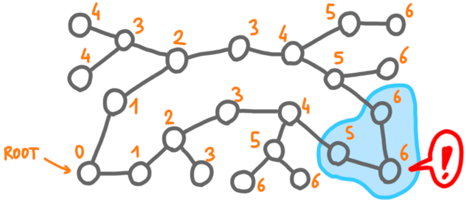
Example and definition

Example: Checking acyclicity.



Example and definition

Example: Checking acyclicity.



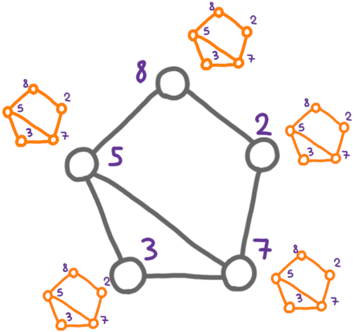
Definition: A local certification consists in a local decision algorithm (A: neighborhood $\mapsto$ accept/reject) such that:

- For all correct configuration: there exists a labeling such that all nodes accept.
- For all incorrect configuration: for all labeling, at least one node rejects.

Certificate size

Key parameter: Maximum size of a certificate (as a function of the network size n). (Memory overhead and measure of locality)

A general upper bound:



[Assume IDs on $O(\log n)$ bits, and unbounded local computation.]

Dichotomy in certificate size

- For any $f(n)$, there exists a property of optimal certificate size $O(f(n))$ (that is, there is no gap).
- But for natural properties, we still witness a dichotomy.

Compact certification (= polylog n size)

- Trees, spanning trees, minimum spanning trees
- planarity, bounded genus, chordal graphs

Polynomial certification (Typically $\Theta(n^2)$ or $\Theta(n)$)

- Symmetry (= having a non-trivial automorphism)
- Diameter $\leq k$
- Triangle-freeness

Dichotomy in certificate size

- For any $f(n)$, there exists a property of optimal certificate size $O(f(n))$ (that is, there is no gap).
- But for natural properties, we still witness a dichotomy.

Compact certification ($=$ polylog n size)

- Trees, spanning trees, minimum spanning trees
- planarity, bounded genus, chordal graphs

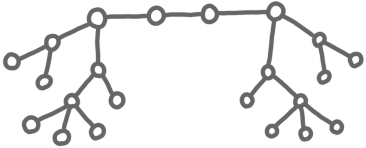
Polynomial certification (Typically $\Theta(n^2)$ or $\Theta(n)$)

- Symmetry ($=$ having a non-trivial automorphism)
- Diameter $\leq k$
- Triangle-freeness

Key question: What can be certified compactly?

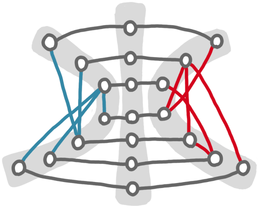
What cannot be certified compactly!

Symmetry (in trees)



- Graphs: trees (simple)
- Property: existence of a non-trivial automorphism (complicated)

Diameter ≤ 3



- Graphs: arbitrary (complicated)
- Property: simple (simply about adjacency)

The model checking approach

$\rightarrow$ Subfield of formal method ; goals: centralized checking that a property holds in a structure (via logic, automata).

Typical theorem shape: All properties expressible in logic X can be *checked efficiently* on the class Y of structures.

Theorems we want: All properties expressible in logic X can be *locally compactly certified* on the class Y of graphs.

Logic on graphs

First-order (FO): Formulas built on:

- $\exists v$, $\forall v$ (quantification on vertices)
- $(u, v) \in E$ (adjacency predicate)
- and, or, etc. (usual connectors)

Monadic second-order (MSO) Formulas built on:

- Same as First-order
- $\exists S$, $\forall S$ (quantification on sets of vertices)

Examples

- Diameter ≤ 3 is in FO:
  $\approx \forall x, \forall y, \exists w_1, \exists w_2, (x, w_1) \in E\ AND\ (w_1, w_2) \in E ...$
- Even-length path is in MSO, but not FO:
  $\approx \exists S, \forall v, \forall u, (u, v) \in E \Rightarrow v \in S, AND\ u \notin S$
  or reverse $+$ conditions on endpoints
- Symmetry is not in MSO: needs quantification on a function

First result: trees and MSO

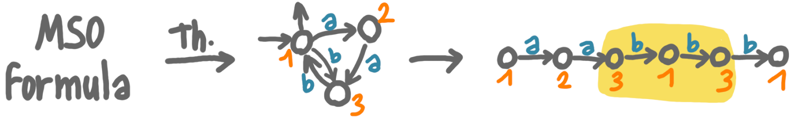
Theorem: In trees, we can certify MSO properties with $O(1)$ bits.

Proof idea: Adapt results from tree automata literature.

Illustration on labeled paths:

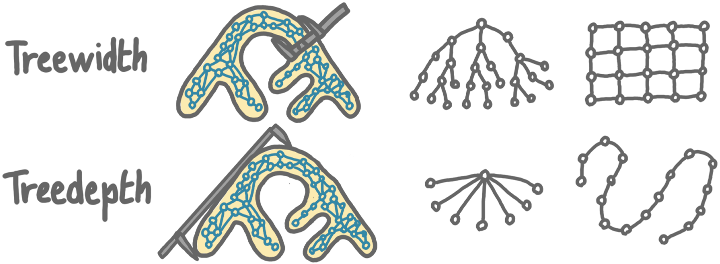
Old theorem: MSO properties on words (= labeled oriented paths) are exactly the languages recognized by finite automata.

How we use it:



Restricting graphs by parameters

Two classic parameters for MSO



Classic theorems:

- MSO property can be checked in time $f(t) \cdot n$ in treewidth-t graphs. (f is huge)
- MSO property can be checked in time $g(t) \cdot n$ in treedepth-t graphs. (g is more reasonable)

Second result: treedepth and MSO

Theorem: MSO properties can be certified with $h(t) \cdot \log n$ bits in graphs of treedepth t.

Treedepth on an example:

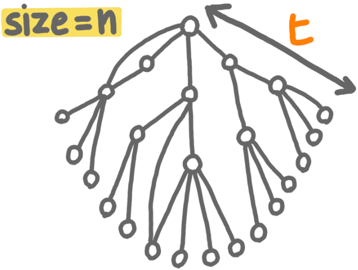
Certification of this structure:

- the list of ancestors in the "tree embedding"
- Check that edges are between ancestors/descendants
- Check consistency (requires some work).

Technique: certified kernelization

Strategy: For a formula $\varphi = \exists x_1, \forall x_2, ...\exists x_k, XXX$

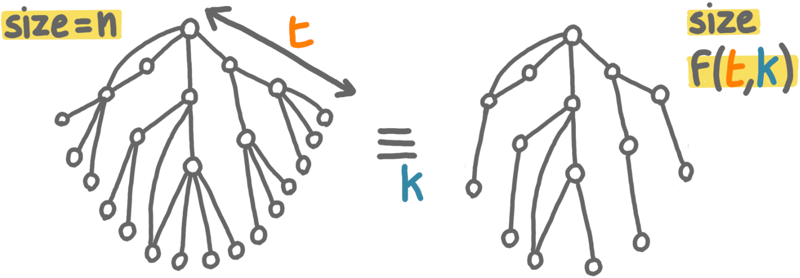
- Find a kernel for MSO of quantifier rank k.
- Certification of φ: give the kernel and its proof to all nodes.



Technique: certified kernelization

Strategy: For a formula $\varphi = \exists x_1, \forall x_2, \ldots \exists x_k, XXX$

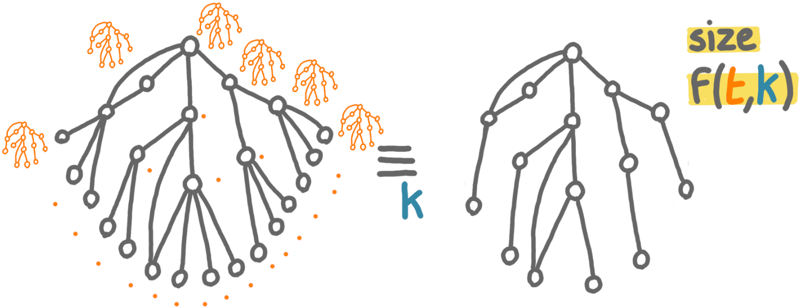
- Find a kernel for MSO of quantifier rank k.
- Certification of φ: give the kernel and its proof to all nodes.



Technique: certified kernelization

Strategy: For a formula $\varphi = \exists x_1, \forall x_2, ...\exists x_{k}, XXX$

- Find a kernel for MSO of quantifier rank k.
- Certification of φ: give the kernel and its proof to all nodes.



Other results and open questions

Further developments:

Fraigniaud, Montealegre, Rapaport and Todinca later proved that the same hold for *treewidth* with $O(\log^2 n)$-bit labels.

Open questions:

- Can we get $O(\log n)$ for treewidth? Or prove a lower bound?
- Other trade-offs between expressivity/structure/certification-size?
- 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
- Memory-efficient self stabilizing protocols for general networks (Afek, Kutten, Young - 1990). doi:10.1007/3-540-54099-7_2
- Locally checkable proofs in distributed computing (Göös, Suomela - 2016). doi:10.4086/toc.2016.v012a019

Tutorial on local certification

- Introduction to local certification (Feuilloley - 2021). doi:10.46298/dmtcs.6280 + Gem talk at PODC (on youtube).

Bibliographic pointers

Certification of planar and bounded-genus graphs

- Compact distributed certification of planar graphs (Feuilloley, Fraigniaud, Montealegre, Rapaport, Rémila, Todinca, 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

- Approximate proof-labeling schemes (Censor-Hillel, Paz, Perry - 2020) doi:10.1016/j.tcs.2018.08.020

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, Todinca - 2022)