Graph Theory in Coq: Minors, Treewidth, and Isomorphisms

Christian Doczkal* Damien Pous*

Univ Lyon, CNRS, ENS de Lyon, UCB Lyon 1, LIP, France

Abstract

We present a library for graph theory in Coq/Ssreflect. This library covers various notions on simple graphs, directed graphs, and multigraphs. We use it to formalise several results from the literature: Menger's theorem, the excluded-minor characterization of treewidth-two graphs, and a correspondence between multigraphs of treewidth at most two and terms of certain algebras. This is the continuation of the work we published at ITP 2018 and we want to report on the advances made since then.

1 Introduction

Given the importance of graph theory and graph algorithms in mathematics and computer science, there are relatively few formalizations of graph theory related results in interactive theorem provers. Moreover, the majority of these deal with the formalization of some particular graph algorithm (e.g. [9]), and as such neither need nor prove more abstract graph theory results. Notable exceptions are the formalization of the four-color theorem in Coq [6] and the formal proof of the Kepler conjecture in HOL-light and Isabelle/HOL [8]. Nevertheless, a general purpose graph library in currently missing in Coq.

We started to develop such a library with the goal of verifying an axiomatizability result for graph isomorphism for a particular class of graphs [3]. Our graph library [2] has been considerably extended and revised during the preparations of the recently submitted extended journal version [5] of [3]. The library deals with simple graphs, directed graphs, and multigraphs; it currently includes basic notions like paths, trees, subgraphs, separators, and isomorphisms, as well as a few more advanced ones: minors and treewidth, whose theory was, to the best of our knowledge, not formalized before. We use the library to formalize three distinct results: Menger's theorem, the excluded-minor characterization of treewidth-two graphs, and a correspondence between multigraphs of treewidth at most two and terms of certain algebras.

2 Recent Additions to the Library

The first main addition to the library since [3] is Menger's theorem; it states that if one needs to remove at least n vertices to disconnect two sets of vertices A and B of some graph, then there exist n pairwise disjoint paths from A to B. Diestel [1, p. 50] calls Menger's Theorem one of the cornerstones of graph theory, and the theorem provides a good test-case for our graph library: it admits a very short paper proof [7], but it nevertheless requires tools to work efficiently with several basic concepts like paths (including collections of paths), and deleting vertices and edges from graphs. We prove the directed vertex version of Menger's theorem and use it to derive several variants and a number of other corollaries (e.g., Hall's marriage theorem) on simple graphs as well as multigraphs. This ensures that our formulation of the theorem is general enough and that our infrastructure makes it possible to transfer results between different kinds of graphs with minimal effort. Within the library, Menger's theorem is used twice: within a new and simpler proof of excluded-minor characterization of treewidth two and to simplify the correctness proof of a function extracting term-descriptions from certain graphs (defined in [3]).

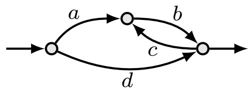
The second main addition is a library for reasoning about bijections between finite types and isomorphisms between graphs. We define a *type* of graph isomorphisms (rather than merely the "is isomorphic to" relation). This allows us to define various constructions on isomorphisms and reason compositionally. In the library, we use this to give a formal proof of the soundness of an axiomatization of graph isomorphism for the graphs described using the aforementioned term language:

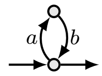
$$u, v, w ::= u{\cdot}v \mid u \parallel v \mid u^\circ \mid \mathrm{dom}(u) \mid 1 \mid \top \mid a \qquad (a \in \Sigma)$$

The syntax describes *2p-graphs*, i.e., edge-labeled multigraphs with two distinguished vertices called *input* and *output*. The binary operations of the syntax correspond to *series* and *parallel* composition. The *converse* operation ($\_^\circ$) swaps input and output and $\mathrm{dom}(\_)$ relocates the output to the input.

*This work has been funded by the European Research Council (ERC) under the European Union's Horizon 2020 programme (CoVeCe, grant agreement No 678157), and was supported by the LABEX MILYON (ANR-10-LABX-0070) of Université de Lyon, within the program "Investissements d'Avenir" (ANR-11-IDEX-0007) operated by the French National Research Agency (ANR).

The constant 1 represents the graph with just a single vertex; $\top$ is the disconnected graph with two vertices (one being the input and the other the output); letters represent single edges. For instance, the graphs of the terms $a{\cdot}(b \parallel c^\circ) \parallel d$ and $1 \parallel a{\cdot}b$ are given on the right. The graph on the bottom is also represented by the term $\mathrm{dom}(a \parallel b^\circ)$. Sequential compositions of graphs can be understood as taking the disjoint union of two graphs and then identifying the output of the first with the input of the second. In Coq, we implement the latter using a *quotient operation* $G_{/\approx}$, merging vertices according to an equivalence relation.





We show that 2p-graphs form a 2p-algebra, i.e., we prove that the operations preserve isomorphisms, and satisfy the twelve axioms of 2p-algebras [10]. That is, we show laws such as $1 \parallel F{\cdot}G \simeq \mathrm{dom}(F \parallel G^\circ)$, where F and G are 2p-graphs and $\simeq$ denotes isomorphisms of 2p-graphs. The proofs proceed by lifting quotients to the top and combining successive quotient operations using lemmas such as:

Lemma 1 *1.* $F + G_{/\approx} \simeq (F+G)_{/\approx'}$ *where* $\approx$ *is an equivalence relation on* G *and* $\approx'$ *is its extension to* $F+G$ *(leaving all vertices of* F *in singleton classes).*

2. $(F_{/\approx})_{/\approx'} \simeq F_{/\approx''}$*, where* $\approx$ *is an equivalence relation on* F*,* $\approx'$ *is an equivalence relation on* $F_{/\approx}$*, and* $\approx''$ *is the equivalence relation on* F *obtained by composing* $\approx$ *and* $\approx'$*.*

For the quotients arising in this application, we can maintain explicit lists of pairs to be identified. Thus, once all disjoint unions have been aligned and all quotients have been lifted to the top, we can use a custom tactic to show that the resulting equivalence relations are (extensionally) equal and therefore yield isomorphic graphs. This compositional treatment modularizes and drastically simplifies the treatment of graph isomorphism compared to [3].

3 Future Work

Currently, the our library contains about 300 definitions and almost 1000 lemmas ($\approx$ 10K lines of code). While the library already contains a number of standard theorems from graph theory, its development is driven by the desire to formalize the axiomatizability result for graph isomorphism [10]. In particular, the current focus is on formalizing completeness of the axiomatization along the lines of [4].

In order to establish this graph library as generally useful, more diverse case studies – including both mathematical theorems and verified algorithms – would need to be carried out. For this we would like to gather feedback from the community as to what features to add or improve in order to make the library useful for a wider audience.

References

1. R. Diestel. *Graph Theory (2nd edition)*. Graduate Texts in Mathematics. Springer, 2000.
2. Christian Doczkal, Guillaume Combette, and Damien Pous. Coq formalization accompanying this paper. https://perso.ens-lyon.fr/damien.pous/covece/graphs/.
3. Christian Doczkal, Guillaume Combette, and Damien Pous. A formal proof of the minor-exclusion property for treewidth-two graphs. In Jeremy Avigad and Assia Mahboubi, editors, *Interactive Theorem Proving (ITP 2018)*, volume 10895 of *LNCS*, pages 178–195. Springer, 2018.
4. Christian Doczkal and Damien Pous. Treewidth-two graphs as a free algebra. In *MFCS*, volume 117 of *LIPIcs*, pages 60:1–60:15. Dagstuhl, 2018.
5. Christian Doczkal and Damien Pous. Graph Theory in Coq: Minors, Treewidth, and Isomorphisms. working paper or preprint, May 2019.
6. Georges Gonthier. Formal proof – the four-color theorem. *Notices Amer. Math. Soc.*, 55(11):1382–1393, 2008.
7. Frank Göring. Short proof of Menger's theorem. *Discrete Mathematics*, 219(1-3):295–296, 2000.
8. Thomas C. Hales, Mark Adams, Gertrud Bauer, Dat Tat Dang, John Harrison, Truong Le Hoang, Cezary Kaliszyk, Victor Magron, Sean McLaughlin, Thang Tat Nguyen, Truong Quang Nguyen, Tobias Nipkow, Steven Obua, Joseph Pleso, Jason Rute, Alexey Solovyev, An Hoai Thi Ta, Trung Nam Tran, Diep Thi Trieu, Josef Urban, Ky Khac Vu, and Roland Zumkeller. A formal proof of the Kepler conjecture. *CoRR*, abs/1501.02155, 2015.
9. Peter Lammich and S. Reza Sefidgar. Formalizing the Edmonds-Karp algorithm. In Jasmin Christian Blanchette and Stephan Merz, editors, *Interactive Theorem Proving (ITP 2016)*, volume 9807 of *LNCS*, pages 219–234. Springer, 2016.
10. Enric Cosme Llópez and Damien Pous. K4-free graphs as a free algebra. In *MFCS*, volume 83 of *LIPIcs*, pages 76:1–76:14. Dagstuhl, 2017.