Coq formalization of graph transformation

Russ Harmer & Damien Pous (Équipe Plume, LIP, ENS Lyon)

Context

Algebraic graph rewriting, also known as graph transformation, is a mathematical theory that specifies how graphs can be rigorously and systematically modified by combinations of well-defined primitive operations. These always include the addition or deletion of nodes and edges but may additionally propose more sophisticated operations such as the cloning or merging of nodes and edges as well as more specific operations to modify accessory data in a graph such as the values of properties/attributes. This theory finds application in a diverse range of situations: it is widely used in model-based software engineering, provides foundations for graph-based databases and the manipulation of string diagrams, generalizes Chomsky grammars to non-linear structures and can be used to specify the evolution of complex systems—and thus serve as the basis of the static/causal analysis and/or stochastic simulation of such systems—as found in organic chemistry, molecular biology and so on.

The theory of algebraic graph rewriting is based on the theory of categories. In the last 15 years or so, a number of distinct, but closely related, categorical theories have been proposed that can be formulated autonomously of category theory itself: in effect, they provide the means to perform higher-level diagrammatic reasoning, in terms of a relatively small collection of inference rules, of a kind that suffices to formulate the key concepts and theorems of the usual variants of graph rewriting, i.e. the so-called double push-out (DPO) and sesqui-push-out (SqPO) approaches. These rules are built on top of category theory—and require knowledge of that theory to prove their correctness—but can be used without knowledge of that theory. In effect, they provide an intermediate language in which we can formalize and prove statements about the theory of graph transformation.

Objectives

The initial objective of this internship is to develop a formalization in Coq of one, or more, of these intermediate level categorical theories of diagrammatic reasoning — this could be quasi-topoi, adhesive categories or rm-quasi-adhesive categories [1] — to provide a basis for the formalization of the core of the theory of DPO and SqPO graph rewriting. This would be followed by the formalization of some key results such as the concurrency theorem [2] and/or the development in Coq of specific concrete graph settings — such as directed multi-graphs or simple graphs — together with proofs that they satisfy appropriate required intermediate language properties. This could open up the possibility of extracting concrete algorithms for graph transformation using SMT solvers, such as Z3, along the lines of [3].

Prerequisites

Specific knowledge of graph transformation is not necessary for this internship. However, some familiarity with elementary category theory (limit and co-limits) and a proof assistant, preferably Coq, would be a considerable advantage.

References

[1] Garner R, Lack S. On the axioms for adhesive and quasi-adhesive categories. Theory and Applications of Categories. 2012;27(3):27-46.

[2] Behr N, Harmer R, Krivine J. Concurrency Theorems for Non-linear Rewriting Theories. In 14th International Conference on Graph Transformation (ICGT 2021), pp. 3-21. Springer, Cham (2021).

[3] Behr N, Heckel R, Ghaffari Saadat M. Efficient computation of graph overlaps for rule composition: theory and Z3 prototyping. In 11th International Workshop on Graph Computational Models (GCM 2020). EPTCS 330:126–144 (2020).