Verified Synthesis of (Very Simple) Sahlqvist Correspondents via Coq

Caitlin D'Abrera
Research School of Computer Science
The Australian National University *
Canberra, Australia

Rajeev Goré
Research School of Computer Science
The Australian National University
Canberra, Australia

Sahlqvist's correspondence theorem [7] is a fundamental theorem of modal logic that sheds light on the expressivity of modal logic with respect to first-order logic. We present a Coq [4] formalisation of this theorem for the "very simple Sahlqvist" class of modal formulae[1][2], which is part of a broader project of formalising the correspondence theorem for the full Sahlqvist class.

In order to state and prove the main theorem, we have produced Coq libraries for reasoning about deeply embedded modal formulae and the relevant fragments of first- and second-order logic used in the theorem statement and proof. In particular, we define our own deep embeddings of monadic first-order logic with a single binary predicate R and equality along with its second-order counterpart, and prove many rudimentary lemmas needed to use these logics. We adopt an elementary approach and discuss several benefits and challenges that come with this design choice.

Moreover, the famous theorem states that first-order correspondents are effectively computable from their (very simple) Sahlqvist counterparts, which is an attribute that features more broadly in modal correspondence theory. This computational aspect has led to various algorithms and implementations being developed. One popular approach that Sahlqvist utilises is second-order quantifier elimination, an area that has progressed independently of this application to modal logic. Implementations of this method include DLS [1], SCAN [5, 6] and SQEMA [2]. Other approaches in correspondence theory include employing algebraic tools, as does the more recent ALBA [3].

Given the algorithmic content of correspondence theory, it is striking that there is no known work that utilises proof assistants to either verify the correctness of the algorithms or produce correct implementations. Our work achieves both of these. Our approach is not to state the algorithm explicitly in Coq and then prove its correctness, but rather to state the theorem that has the general form "`forall (A : Modal), exists (B : FirstOrder), ...`"[3] and encode the algorithmic content in the witness for `B` given in the proof that depends on `A`. To do so, we follow the original proof of Sahlqvist's correspondence theorem, thus allowing us to synthesise a Haskell program that computes first-order correspondents given very simple Sahlqvist modal formulae as inputs, automatically produced using Coq's extraction facility.

In light of the lack of work in this area, our contribution paves the way for future formalisation efforts in algorithmic modal correspondence theory to utilise Coq's synthesising capabilities in order to generate verified algorithms that correctly produce correspondents.

References

[1] W. Conradie (2006): *On the strength and scope of DLS*. *Journal of Applied Non-Classical Logics* 16(3-4), pp. 279–296.

*Supported by an Australian Government Research Training Program (RTP) Scholarship.

[1] The final theorem statement is called `vsSahlq_full_Modal` and can be found here: `https://github.com/caitlindabrera/Sahlqvist/tree/master/vsSahlq`.

[2] An earlier version of our code was presented as a short paper at Advances in Modal Logic in 2018.

[3] This is a simplification for the sake of illustrating the process of extraction from the theorem statement. We direct the reader to our code for the full statement.

Submitted to:
LFMTP 2020

[2] W. Conradie, V. Goranko & D. Vakarelov (2006): *Algorithmic Correspondence and Completeness in Modal Logic. I. The Core Algorithm SQEMA*. Logical Methods in Computer Science 2(1).

[3] W. Conradie & A. Palmigiano (2012): *Algorithmic correspondence and canonicity for distributive modal logic*. Annals of Pure and Applied Logic 163(3), pp. 338–376.

[4] The Coq Development Team (2017): *The Coq Proof Assistant Reference Manual, version 8.7*. Available at `http://coq.inria.fr`.

[5] D. Gabbay & H. J. Ohlbach (1992): *Quantifier Elimination in Second-Order Predicate Logic*. In: Proceedings of the Third International Conference of Principles of Knowledge Representation and Reasoning, Morgan Kaufmann, pp. 425 – 436.

[6] V. Goranko, U. Hustadt, R. A. Schmidt & D. Vakarelov (2004): *SCAN is Complete for All Sahlqvist Formulae*. In R. Berghammer, B. Möller & G. Struth, editors: Relational and Kleene-Algebraic Methods in Computer Science, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 149–162.

[7] H. Sahlqvist (1975): *Completeness and Correspondence in the First and Second Order Semantics for Modal Logic*. In S. Kanger, editor: Proceedings of the Third Scandinavian Logic Symposium, Studies in Logic and the Foundations of Mathematics 82, Elsevier, pp. 110 – 143.