Logic and Computation

Matching Plans for Frame Inference in Compositional Reasoning.

Daniele Nantes-Sobrinho
(UNB/Imperial College London)

Wednesday, February 7, 2024.
16h30 - 17h10

Math Department- Mini Auditorium

Abstract.

The use of function specifications and manipulation of user- defined predicates are two essential ingredients of modern compositional verification tools. To execute these operations successfully, these tools must be able to solve the frame inference problem, that is, understand the parts of the state relevant for the operation at hand. We introduce matching plans, which facilitate frame inference and advance the state-of- the-art in that they allow tool users to write intuitive and understandable specifications and the tools to efficiently infer the information required to perform frame inference.

(Joint work with Andreas Lööw, Petar Maksimovic, Philippa Gardner, Sacha Ayoun)

References

[1] aldoni, R., Coppa, E., D'Elia, D.C., Demetrescu, C., Finocchi, I.: A survey of symbolic execution techniques. ACM Computing Surveys 51(3) (2018)

[2] erdine, J., Calcagno, C., O'Hearn, P.W.: Smallfoot: Modular automatic assertion checking with separation logic. In: FMCO. pp. 115–137 (2005)

[3] erdine, J., Calcagno, C., O'Hearn, P.W.: Symbolic execution with separation logic. In: APLAS. pp. 52–68 (2005)

[4] ragoso Santos, J., Maksimović, P., Sampaio, G., Gardner, P.: JaVerT 2.0: Compositional symbolic execution for JavaScript. PACMPL 3(POPL) (2019). https://doi.org/10.1145/3290379

[5] ragoso Santos, J., Maksimović, P., Ayoun, S., Gardner, P.: Gillian, part I: A multi-language platform for symbolic execution. In: Programming Language Design and Implementation (PLDI) (2020). https://doi.org/10.1145/3385412.3386014, https://doi.org/10.1145/3385412.3386014

[6] acobs, B., Smans, J., Piessens, F.: The VeriFast Program Verifier: A Tutorial (2017). https://doi.org/10.5281/ZENODO.1068185

[7] ., Summers, A.J.: An automatic encoding from VeriFast predicates into implicit dynamic frames. In: Verified Software: Theories, Tools, Experiments (2014). https://doi.org/10.1007/978-3-642-54108-7_11

[8] aksimović, P., Ayoun, S., Santos, J.F., Gardner, P.: Gillian, part II: Real-world verification for JavaScript and C. In: Computer Aided Verification (CAV) (2021). https://doi.org/10.1007/978-3-030-81688-9_38, https://doi.org/10. 1007/978-3-030-81688-9_38