A Modular Implementation of $L^\star$ in Rust

Olivier Levillain

2023-2024

Network protocols are pervasive in our digital usages, and should thus be secure to ensure the security and the privacy of our systems and data.

One way to study these protocols is the black-box state-machine inference approach proposed in 1987 by Angluin with his algorithm $L^\star$ [Ang87][1] We have already studied different protocols (TLS [RLD22], SSH, OPC-UA) at Télécom SudParis, and we believe we could systemize our approach more.

To this aim, we would like to have a proper, modular and efficient implementation of the $L^\star$ algorithm in Rust. Indeed the ideal implementation would have the following properties:

- be able to infer both regular languages (finite state automata) and Mealy machines;
- accept various equivalence methods to be plugged in easily;
- allow for fine-grained monitoring of the inference process to help us understand how to increase the performance;
- include the ability to monitor the target implementation being infered in real-time, switching from a pure black-box model to a greyish one.

The steps for this project would probably be the following ones:

- read and understand articles about $L^\star$ and its applications;
- design a proper and modular inference engine;
- write the code;
- test the engine on various use cases (including both a deterministic finite automaton and a Mealy machine).

If the progress is fast, extensions could be imagined:

- write different equivalence methods and test their performance;
- implement the grey-box approach on a real-world use-case.

Expected Deliveries

The main expected deliverables are the design rationale of the engine, and the corresponding code.

Prerequisites

- Notions of Rust programming;
- Basic Knowledge of Graphs and DFAs;
- Systems and Network skills will also be useful.

[1] To be precise, Angluin described an algorithm to infer regular languages/automata, whereas this project is about Mealy machine inference, but an extension was later devised.

Logistics

Regular meetings will be scheduled with the advisor, either via visioconference or in Palaiseau. If you are interested, send an email to (`olivier.levillain@telecom-sudparis.eu`).

References

[Ang87] Dana Angluin. Learning regular sets from queries and counterexamples. *Inf. Comput.*, 75(2):87–106, 1987.

[RLD22] Aina Toky Rasoamanana, Olivier Levillain, and Hervé Debar. Towards a Systematic and Automatic Use of State Machine Inference to Uncover Security Flaws and Fingerprint TLS Stacks. In *27th European Symposium on Research in Computer Security, ESORICS 2022, Copenhagen, Denmark*, pages 637–657, September 2022.