Formal Verification (CS-550) : Background paper and project summary, October 23rd 2020

Formal verification and compression/encoding algorithms

Group members

- Samuel CHASSOT 270955
- Daniel Filipe NUNES SILVA 275197

Main paper

Senjak, Christoph-Simon; Hofmann, Martin (2016): An Implementation of Deflate in Coq. In: Fitzgerald, John (Hrsg.): FM 2016. Cyprus

Work

We plan to first read, understand and present our paper which is about rigorously describing compression/encoding algorithms and formalizing them in Coq.

We will then start by implementing a basic algorithm like Lempel-Ziv or Huffman coding in Scala. Those seem relevant considering our paper.

Finally, we want to use stainless, as we feel more confortable with it than we do with Coq, to verify some properties of our implementation. Those properties will certainly become clearer as we will study the reference paper. As mentioned by Prof. Kuncak during our meeting, the structure of this implementation may be similar to Lab 2, namely the tokenizer. Such compression/encoding algorithms can indeed be seen as a tokenizing and a pretty-printing operation. That makes us confident about Stainless being a workable solution for this case study.

Orgnaization

Workload   As we are two students in our group, we will be splitting the work equally as we progress through this project.

Plan

- Week 7 : Read and understand the paper.
- Week 8 : Prepare and record the presentation.
- Week 9 : Implement the most relevant algorithm related to our paper.
- Week 10 : Select the properties we want to verify and start proving them.
- Week 11 : Continue proving the stated properties.
- Week 12 : Depending on our progress, we could either go further in the properties we want to prove or adapt our algorithm to deal with more sophisticated data types or even turn our verifier algorithm into a runnable program to run with files as inputs and outputs.
- Week 13 : Prepare and record the final presentation.
- Week 14 : Finalize our work and write the final report.