Massachusetts Institute of Technology
Department of Electrical Engineering and Computer Science

Proposal for Thesis Research in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Title: Performance Engineering of Proof-Based Software Systems

Submitted by: Jason Gross
258 Prospect St, #1L
Cambridge, MA 02139

(Signature of Author)

Date of Submission: June 17, 2020

Expected Date of Completion: September—December 2020

Laboratory: Computer Science and Artificial Intelligence Laboratory

Brief Statement of the Problem:

The proposed research is a study of performance issues that come up in engineering large-scale proof-based systems in Coq. The thesis presents lessons learned about achieving acceptable performance in Coq in the course of case-studies on formalizing category theory, developing a parser synthesizer, and constructing a verified compiler for synthesizing efficient low-level cryptographic primitives. We also present a novel method of simple and fast reification, and a prototype tool for faster rewriting and customizable reduction which does not require extending Coq's trusted code base.