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.