# Algorithmic Software Verification Project

Argonne National Laboratory Proposal no. 93079
ONR Reference 5000 - 1133/93/A0068
Office of Naval Research R & T 4331018srp01

Ewing L. Lusk
Mathematics and Computer Science Division
Argonne National Laboratory
Argonne, IL 60439
Tel: (708) 252-7852
FAX: (708) 252-5986
Email: lusk@mcs.anl.gov

## Summary

This proposal is for first-year funding to start the QED Project to formalize and verify a significant body of mainstream mathematics. The basic activities to be funded are:

- a workshop to collect ideas, achieve necessary consensus, and formulate a plan of action,
- travel to facilitate collaboration by the initial set of principal implementors, and
- dissemination of the concept and initial results in order to attract more participants.

The total budget proposed here is $58,466.

## QED Project Summary

The aim of the QED project is to build a single, distributed, computerized repository that rigorously represents all important, established mathematical knowledge. The construction of this system will be a scientific undertaking of significant proportions, requiring the co-operation of many mathematicians, computer scientists, research groups, research agencies, universities, and corporations. This system will have benefits for mathematics, science, technology, and education.

**Benefits.** For mathematicians and scientists, the QED system will provide a mechanically checked basis for reliably building the edifice of mathematics far beyond the detailed comprehension of any single individual. For those developing high technology systems, the QED system will provide not only precisely developed mathematical theories of materials but also tools for the development of theorems about the mathematical control of systems, theorems whose detailed proofs it seems beyond the attention span of humans to construct with high reliability. For students, the QED system will provide an interactive mechanism for investigating the entirety of mathematics cast in a coherent framework.

**Historical background.** The work of many well-known logicians has established that mathematics can be rigorously checked by machine. The work of dozens of research groups throughout the world has repeatedly established that many substantial parts of mathematics can be rigorously incorporated into computer systems.

**Criticism of the status quo.** The efforts of the many, rather small research groups working in such varied areas as symbolic algebra, program verification, and automated reasoning can be criticized for making rather slow progress towards the goal of building a single system that contains all important mathematical knowledge. This slow pace can be attributed to many factors including (a) duplication of efforts due to a plethora of logics and projects, (b) lack of reasoned appreciation of the necessity of large-scale cooperation in the achievement of the QED objective, and (c) a primary focus on other objectives, for example upon automating a small, particular part of mathematics or upon the automation of the discovery of difficult, new theorems.

**Connections with existing programs.** We can distinguish four areas of ongoing activity related in some sense to the QED project: (A) Internationally, there are perhaps several dozen small, but significant, projects involved in automated reasoning and in mechanical hardware or software verification. Communication between these groups is better than one might expect given their extremely varied objectives and sources of financial support, but actual cooperation between these groups is relatively small. (B) There are many incompatible symbolic algebra projects, including some well-known commercial systems: Macsyma, Maple, and Mathematica. (C) The numerical analysis community has developed well-known standard software systems, e.g., LINPACK. (D) Increasingly, the regular pure mathematics community is using computers in the investigation of mathematical conjectures. To the best of our knowledge, between these four areas there is only slight communication and minor cooperation. The QED project can provide a unifying focus for all projects in these areas.

**Connections with other current technical objectives.** The QED project is aligned with a number of objectives currently supported by the U. S. government and the computer science community.

**Electronic libraries** The development of a library of mathematical knowledge heavily overlaps with the QED project. Clearly, an electronic mathematical library need, per se, put no more emphasis upon syntactic uniformity, formality, or rigor than one finds in the ordinary mathematical literature. However, the acquisition and organization of important mathematical knowledge in mechanical form will obviously be a crucial part of the QED project.

**Software repositories** Among the many concepts and theorems in the QED database will be the definitions of and proofs of correctness of many common algorithms and computer systems, including compilers and operating systems.

**Verifiably correct software** The verification of software is the major imagined practical application of QED. Especially important to the future of verification is the QED codification of analysis, which will permit the specification of safety-critical systems.

**Megaprogramming** The exact mathematical specification of the software proved the in the QED database will permit the reliable, provable interconnection of standard software components to produce specialized applications aat a fraction of the cost of building such systems from scratch, which is the current practice.

**Information highways and HPCC results** Key to QED's success will be the wide collaboration of hundreds of mathematicians modifying and accessing a database of many gigabytes. The HPCC networking and database goals are ideal to support the development of QED.

## What's Needed Next

So far, progress has been confined to a gradual, informal discussion of the project's goals. A public mailing list (`qed@mcs.anl.gov`) has been set up at Argonne which currently has 146 members. Discussion has just begun on what might serve as the base logic for the implementation of the system. A full description of the goals of the QED project can be found in "The QED Manifesto", available through the mailing list.

We need to turn QED from an intriguing idea into a real project. The first decision needed is a consensus on the underlying logic, followed by an implementation development plan. In our opinion the best way to accelerate this process is to hold a workshop at which alternatives can be examined and a decision reached. (Email promotes discussions but not decisions.) The final phase of the workshop would be the adoption of an implementation plan. The principal implementors will need to meet and travel funds for them to do so are requested.

We propose to hold a three-day workshop at Argonne National Laboratory in the early fall, in order to allow for planning by the people we would hope could plan to attend. Argonne would contribute the facilities and administration costs.

## Potential Workshop Participants

In order to give an accurate impression of who might be involved, we include here a list of those we would plan to invite to the initial workshop. No doubt this is list is incomplete, and the continuing email discussion will reveal some new names to us.

| | |
|---|---|
| Robert Boyer | <boyer@cli.com> |
| Rod Burstall | <rb@lfcs.edinburgh.ac.uk> |
| N. de Bruijn | <wsdwnb@win.tue.nl> |
| Hank Barendregt | <henk@cs.kun.nl> |
| Michael Beeson | <beeson@cats.ucsc.edu> |
| Rod Burstall | <rb@lfcs.edinburgh.ac.uk> |

| | |
|---|---|
| Sol Feferman | <sf@csli.stanford.edu> |
| Mike Gordon | <Mike.Gordon@cl.cam.ac.uk> |
| Gerard Huet | <Gerard.Huet@inria.fr> |
| Matt Kaufmann | <kaufmann@cli.com> |
| Ewing Lusk | <lusk@mcs.anl.gov> |
| Ian Mason | <iam@cs.stanford.edu> |
| David McAllester | <dam@ai.mit.edu> |
| Sean Matthews | <sean@mpi-sb.mpg.de> |
| Bill McCune | <mccune@mcs.anl.gov> |
| Dale Miller | <dale@saul.cis.upenn.edu> |
| J Moore | <moore@cli.com> |
| David Mumford | <mumford@das.harvard.edu> |
| Bengt Nordstrum | <bengt@cs.chalmers.se> |
| Ross Overbeek | <overbeek@mcs.anl.gov> |
| Gordon Plotkin | <gdp@lfcs.edinburgh.ac.uk> |
| Joerg Siekmann | <siekmann@dfki.uni-sb.de> |
| Mark Stickel | <Stickel@ai.sri.com> |
| Carolyn Talcott | <clt@cs.stanford.edu> |
| Javier Thayer | <jt@linus.mitre.org> |
| Randy Pollack | <rap@dcs.edinburgh.ac.uk> |
| Richard Waldinger | <waldinger@ai.sri.com> |
| Larry Wos | <wos@mcs.anl.gov> |

## Budget

This is an approximate budget for the workshop, post-workshop participant travel, and a half-month each of salary for the P.I.'s.

| | |
|---|---|
| Workshop for 20 participants: | |
| Travel: 12 domestic @ $750 | 9,000 |
| Travel: 8 foreign @ $1500 | 12,000 |
| Lodging: 20 x $50 x 3 | 3,000 |
| Per Diem: 20 x $20 x 3 | 1,200 |
| | 25,200 |
| Overhead: 32.8% | 8,266 |
| Total for workshop: | 33,466 |
| Travel (overhead included) | 10,000 |
| 1/2 month Boyer (overhead included) | 7,500 |
| 1/2 month Lusk (overhead included) | 7,500 |
| Total: | 58,466 |

**Travel detail.** The travel budget is for post-workshop travel to ensure close cooperation among the various implementors, as well as to publicize the project in the mathematical community. We envision that each of the two P.I.'s will need to make one international trip ($2,000) and three domestic trips ($1000). The most likely sites to visit are INRIA in France, Edinburgh, MIT, Berkeley, Stanford (and SRI), USC, and the University of Pennsylvania. Thus the $10,000 in the above budget breaks down as follows:

| | |
|---|---|
| Trip to INRIA | 2,000 |
| Trip to Edinburgh | 2,000 |
| 2 trips to MIT | 2,000 |
| Trip to Berkeley | 1,000 |
| Trip to Stanford & SRI | 1,000 |
| Trip to USC | 1,000 |
| Trip to Penn | 1,000 |
| Total: | 10,000 |

**How to spend less:** The first thing to go should definitely be the funding for the P.I.'s, on the grounds that it will be a labor of love for them. Next, one could reduce the amount of unspecified post-workshop travel funding, on the grounds that the project will be close enough to the main area of each participant that he can use his own normal research funding sources for the purpose of the QED collaboration. Finally, one could have fewer people at the workshop.