QED: A grand unified theory?

John Harrison

Intel Corporation

18th July 2014 (09:00–09:35)

14th March 1993: The QED mailing list

```
To: avenhaus@de.uni-kl.informatik, bibel@de.th-darmstadt.informatik.intellektik,
    bledsoe@edu.utexas.cs, boyer@com.cli, bundy@uk.ac.ed,
    burghard@de.gmd.karlsruhe, caferra@fr.imag.cosmos,
    dahn@de.hu-berlin.informatik.hubinf, denzinge@de.uni-kl.informatik,
    ...
    sf@edu.stanford.csli, kaufmann@com.cli, moore@com.cli,
    Mike.Gordon@uk.ac.cam.cl, Gerard.Huet@fr.inria, lipman@MIL.NAVY.ONR-HQ,
    nancym@edu.washington.u, iam@edu.stanford.cs, sean@de.mpg.mpi-sb,
    mumford@edu.harvard.das, bengt@se.chalmers.cs, shankar@com.sri.csl,
    clt@edu.stanford.cs, jt@org.mitre.linus, rap@uk.ac.ed.dcs,
    wachter@edu.umd.cs, wos@gov.anl.mcs, overbeek@gov.anl.mcs, lusk@gov.anl.mcs
Subject: Invitation to join the QED mailing list
Date: Sun, 14 Mar 1993 15:51:09 -0600
From: Rusty Lusk <lusk@gov.anl.mcs>

This is an invitation from Bob Boyer (and me) to join a public mailing list
for the QED project.  The list is for the discussion of the QED project for
the verification of a significant body of mathematical thought, based on a
minimal set of logical first principles.  A more detailed ddescription of the
project's goals can be obtained by anonymous ftp from info.mcs.anl.gov.  Take
the file "manifesto" from the directory pub/qed.

To join the list, send mail to Majordomo@mcs.anl.gov containing the message

  subscribe qed

If you would like to specify an email address instead of letting it default to
the one you are sending from, use the form

  subscribe qed foo@bar.bazz.fazz
```

14th March 1993: The QED mailing list

```
Subject: Invitation to join the QED mailing list
Date: Sun, 14 Mar 1993 15:51:09 -0600
From: Rusty Lusk <lusk@gov.anl.mcs>

This is an invitation from Bob Boyer (and me) to join a
public mailing list for the QED project.  The list is
for the discussion of the QED project for the
verification of a significant body of mathematical
thought, based on a minimal set of logical first
principles.  A more detailed ddescription of the
project's goals can be obtained by anonymous ftp from
info.mcs.anl.gov.  Take the file "manifesto" from the
directory pub/qed.
```

The QED Manifesto

Later published in CADE-12 (Springer LNCS vol. 813, pp. 238-251, 1994).

> *QED is the very tentative title of a project to build a computer system that effectively represents all important mathematical knowledge and techniques. The QED system will conform to the highest standards of mathematical rigor, including the use of strict formality in the internal representation of knowledge and the use of mechanical methods to check proofs of the correctness of all entries in the system.*

See `ftp://info.mcs.anl.gov/pub/qed/manifesto.aug-93`

QED Manifesto: Critique of current efforts

1. Too much code to be trusted.
2. Too strong a logic.
3. Too limited a logic.
4. Too unintelligible a logic.
5. Too unnatural a syntax.
6. Parochialism.
7. Too little extensibility.
8. Too little heuristic search support.
9. Too little care for rigor.
10. Complete absence of inter-operability.
11. Too little attention paid to ease of use.

QED Manifesto: A root logic as the basis for sharing

An important early technical step will be to “get off the ground”, logically speaking, which we will do by rooting the QED system in a “root logic”, whose description requires only a few pages of typical logico-mathematical text.

QED Manifesto: A root logic as the basis for sharing

An important early technical step will be to "get off the ground", logically speaking, which we will do by rooting the QED system in a "root logic", whose description requires only a few pages of typical logico-mathematical text.

The logic will, by necessity, be sufficiently strong to check any explicit computation, but the logic surely must not prejudge any historically debated questions such as the law of the excluded middle or the existence of uncountable sets.

QED Manifesto: A root logic as the basis for sharing

An important early technical step will be to “get off the ground”, logically speaking, which we will do by rooting the QED system in a “root logic”, whose description requires only a few pages of typical logico-mathematical text.

The logic will, by necessity, be sufficiently strong to check any explicit computation, but the logic surely must not prejudge any historically debated questions such as the law of the excluded middle or the existence of uncountable sets.

As just one hint of a logic that might be used as the basis of QED, we mention Primitive Recursive Arithmetic (PRA) which is the logic Skolem invented for the foundations of arithmetic, which was later adopted by Hilbert-Bernays as the right vehicle for proof theory [. . .] its inductive power permits the proof of metatheorems

QED mailing list discussion topics

See `http://mizar.org/qed/` for links to archive

- Let's start
- the base logic
- a multilingual approach
- goals and the base logic
- Bourbaki/Mathias
- Verification systems
- "Little Theories" and the base logic
- Answer to a question, and further speculation on a QED foundation
- Feferman FSO reference
- little theories and encryption
- Different Schools
- illusion
- Machine Math
- Why should a mathematician be interested in QED?
- Machine math, clarification

QED message from Boyer (6th August 1993)

> Indeed, there have been a good number of QED-like efforts spread over at least the last 27 years, both large scale and small. (I hear rumors that the Polish MIZAR effort may be the largest so far.) But one can ask the question whether any of the efforts now underway has sufficient support to achieve coverage of the most commonly used sorts of mathematics.
>
> We not only have *some* proof checking systems, we may have a Babel's worth of them. I doubt whether this plethora of really wonderful alternative proof-checking systems is appealing to the various funding agencies or to potential users. People seemed to tire of inventing new programming languages sometime around 1980 or so. Maybe some day the C and FORTRAN of proof checking systems will become clear. (That was a joke.)

QED Workshop I (Argonne, 18–20 May 1994)

Report on the workshop

You can find a formal report on the workshop, synthesized by Gail Pieper, as Argonne technical report ANL/MCS-TM-191, here:

`ftp://info.mcs.anl.gov/pub/tech_reports/reports/TM191.pdf`

This includes various concrete information like a list of participants (Thomas Jech was there) and the main topics of discussion.

> *The most important conclusion drawn at the QED Workshop was that* QED is an idea worth pursuing*, a statement with which virtually all participants agreed.*

What follows is a collection of my own informal recollections as recounted in an email to a colleague at the time.

My informal report on the workshop (1)

We spent about a day aimlessly discussing miscellaneous issues. Chet [Murthy] was trying to push the idea of a project simply to translate between different systems. The main discussion was about Mizar; indeed there seemed to be a body of opinion (including surprising people like Paul Jackson – I thought he believed in constructive type theory) to simply base the QED project on (a reengineered) Mizar.

My informal report on the workshop (1)

We spent about a day aimlessly discussing miscellaneous issues. Chet [Murthy] was trying to push the idea of a project simply to translate between different systems. The main discussion was about Mizar; indeed there seemed to be a body of opinion (including surprising people like Paul Jackson – I thought he believed in constructive type theory) to simply base the QED project on (a reengineered) Mizar.

Then Bob Boyer presented something quite similar to the original manifesto; i.e. embed object logics in PRA (or something similar with other recursive datatype), write a proof checker in PRA for each particular system, and then try to establish metatheorems of the form "if $\vdash A$ holds in system 1 then $\vdash A'$ holds in system 2".

My informal report on the workshop (2)

Everyone in the room except me seized on this with great enthusiasm. I wasn't necessarily opposed to it, but I wanted some serious discussion. For example, since all intertranslatability proofs are likely to be constructive, what are we really gaining over Chet's idea of simply doing the translation? [. . .] my attempts to introduce sanity (as I see it) into the discussion were all howled down. They weren't interested in the LCF lesson about how much easier it is to write heuristic functions which almost always work than formally verified ones, which bears directly on this issue.

My informal report on the workshop (2)

Everyone in the room except me seized on this with great enthusiasm. I wasn't necessarily opposed to it, but I wanted some serious discussion. For example, since all intertranslatability proofs are likely to be constructive, what are we really gaining over Chet's idea of simply doing the translation? [. . .] my attempts to introduce sanity (as I see it) into the discussion were all howled down. They weren't interested in the LCF lesson about how much easier it is to write heuristic functions which almost always work than formally verified ones, which bears directly on this issue. [. . .] Eventually I realized I was merely irritating people by my contribution so I just gave up.

My informal report on the workshop (3)

That afternoon it was as if nothing had been decided. People started debating user interfaces. I had decided to shut up, but I couldn't contain my incredulity. Eventually I, supported now by Piotr [Rudnicki], Javier [Thayer] and Bill Pase, started trying to get an answer to "what is the user interface to?" Is it to do metaproofs in PRA or in the embedded logic? (Nobody had said anything yet about an actual QED theorem prover!) Nobody seemed to know the answer. Later people started debating whether the base logic should be founded on set theory or type theory. What base logic? Apart from the metalogic of PRA, there is no preferred base logic, according to the debate in the morning. I found the whole thing permeated by an air of total unreality.

My informal report on the workshop (3)

That afternoon it was as if nothing had been decided. People started debating user interfaces. I had decided to shut up, but I couldn't contain my incredulity. Eventually I, supported now by Piotr [Rudnicki], Javier [Thayer] and Bill Pase, started trying to get an answer to "what is the user interface to?" Is it to do metaproofs in PRA or in the embedded logic? (Nobody had said anything yet about an actual QED theorem prover!) Nobody seemed to know the answer. Later people started debating whether the base logic should be founded on set theory or type theory. What base logic? Apart from the metalogic of PRA, there is no preferred base logic, according to the debate in the morning. I found the whole thing permeated by an air of total unreality.

The next day, Michael Beeson provided a good stimulus for actually getting started, though from the silence of the QED list it looks as if nobody took it seriously. I was happy enough to play my part, but it still seemed to me that the so-called "discussion" had been utterly pointless.

My informal report on the workshop (4)

Anyway, on the good side, I met up with a few friends like Chet [Murthy] and Paul Jackson again, and a few interesting new people.

My informal report on the workshop (4)

Anyway, on the good side, I met up with a few friends like Chet [Murthy] and Paul Jackson again, and a few interesting new people.

Most interestingly, got to know two of the key Mizar people, Piotr [Rudnicki] and Andrzej [Trybulec], and we actually had a demo of the Mizar system in the bar. It quite impressed me in some ways – I'll tell you more sometime. They and I had a lot of common ground; in fact we arranged for reciprocal visits Cambridge/Warsaw sometime. Piotr said "anyone who writes HOL scripts is a friend of mine" while Andrzej had this motto (contra automation) "proof is a pleasure that the machine should not deprive us of".

QED Workshop II (Warsaw, 20–22 July 1995)

Agenda for QED II (1)

- Andrzej Trybulec - Computer reconstruction of mathematical technology
- Paul Jackson – Can we agreeably resolve the tension between type theorists (constructivists, de Bruijn, Martin Löf, Constable) and the classical mathematicians?
- Martin Strecker – The organization of a data base of mathematical knowledge
- John Harrison – Reflection: practically necessary or not?
- Randall Holmes – Indeterminateness
- Manfred Kerber – Possible use of already formalized mathematical knowledge

Agenda for QED II (2)

- Javier Thayer – Formalized Analysis
- Peter White – Mathematical synthesis
- Andrzej Trybulec – Syntax vs. semantics
- John McCarthy – Heavy duty set theory
- Piotr Rudnicki – To type or not to type
- Bernd Ingo Dahn – Cooperation of automated and interactive theorem provers
- Deepak Kapur – What are the connections, interrelations, and antipathies between proof checking and automatic theorem proving?
- Manfred Kerber – Why we are needed by mathematics

See `http://mizar.org/people/romat/qed95rep.pdf` for more details.

Twenty years on

Did the QED project itself succeed in its aims?

Twenty years on

Did the QED project itself succeed in its aims?

- In the most obvious sense, not at all.

Twenty years on

Did the QED project itself succeed in its aims?

- In the most obvious sense, not at all.
  - QED list discussion tailed off with no more workshops.

Twenty years on

Did the QED project itself succeed in its aims?

- In the most obvious sense, not at all.
  - QED list discussion tailed off with no more workshops.
  - There is no unified ‘QED system’

Twenty years on

Did the QED project itself succeed in its aims?

- In the most obvious sense, not at all.
  - QED list discussion tailed off with no more workshops.
  - There is no unified 'QED system'
  - There is not much serious use of metalogics to share results

Twenty years on

Did the QED project itself succeed in its aims?

- In the most obvious sense, not at all.
    - QED list discussion tailed off with no more workshops.
    - There is no unified ‘QED system’
    - There is not much serious use of metalogics to share results
    - If anything, Balkanization has got even worse

Twenty years on

Did the QED project itself succeed in its aims?

- In the most obvious sense, not at all.
  - QED list discussion tailed off with no more workshops.
  - There is no unified ‘QED system’
  - There is not much serious use of metalogics to share results
  - If anything, Balkanization has got even worse
- A more positive view

Twenty years on

Did the QED project itself succeed in its aims?

- In the most obvious sense, not at all.
    - QED list discussion tailed off with no more workshops.
    - There is no unified ‘QED system’
    - There is not much serious use of metalogics to share results
    - If anything, Balkanization has got even worse
- A more positive view
    - QED had many positive side-effects like bringing Mizar and other theorem proving groups together

Twenty years on

Did the QED project itself succeed in its aims?

- In the most obvious sense, not at all.
    - QED list discussion tailed off with no more workshops.
    - There is no unified 'QED system'
    - There is not much serious use of metalogics to share results
    - If anything, Balkanization has got even worse
- A more positive view
    - QED had many positive side-effects like bringing Mizar and other theorem proving groups together
    - There has been substantial progress over 20 years in formalizing non-trivial theorems and improving systems.

Twenty years on

Did the QED project itself succeed in its aims?

- In the most obvious sense, not at all.
  - QED list discussion tailed off with no more workshops.
  - There is no unified ‘QED system’
  - There is not much serious use of metalogics to share results
  - If anything, Balkanization has got even worse
- A more positive view
  - QED had many positive side-effects like bringing Mizar and other theorem proving groups together
  - There has been substantial progress over 20 years in formalizing non-trivial theorems and improving systems.
  - We do have a number of working approaches for sharing proofs between theorem-proving systems.

Notable theorems

As well as the landmarks like the Odd Order Theorem and the Kepler Conjecture, which others will describe, many ‘middle-sized’ theorems have been formalized, e.g.

- Gödel’s First Incompleteness Theorem — Natarajan Shankar (NQTHM), Russell O’Connor (Coq)
- Brouwer Fixed Point Theorem — Artur Kornilowicz and Karol Pak (Mizar), John Harrison (HOL Light)
- Jordan Curve Theorem — Tom Hales (HOL Light), Andrzej Trybulec et al. (Mizar)
- Prime Number Theorem — Jeremy Avigad et al (Isabelle/HOL), John Harrison (HOL Light)
- First and second Cartan Theorems — Marco Maggesi et al (HOL Light)
- Gödel’s Second incompleteness Theorem — Larry Paulson (Isabelle/HOL)

Substantial libraries

Many theorem provers have particularly well-developed libraries in certain areas:

- Mizar — Continuous lattices
- HOL Light — Analysis and topology in Euclidean space
- Coq — Mathematical Components

Substantial libraries

Many theorem provers have particularly well-developed libraries in certain areas:

- Mizar — Continuous lattices
- HOL Light — Analysis and topology in Euclidean space
- Coq — Mathematical Components

The very size of such libraries provides much stronger motivation to share results!

Substantial libraries

Many theorem provers have particularly well-developed libraries in certain areas:

- Mizar — Continuous lattices
- HOL Light — Analysis and topology in Euclidean space
- Coq — Mathematical Components

The very size of such libraries provides much stronger motivation to share results!
On the other hand, there are other approaches like hand-translation . . .

Interfaces between interactive provers

Transferring results:

- hol90 → Nuprl: Howe and Felty 1997
- ACL2 → hol90: Staples 1999
- ACL2 → HOL4: Gordon, Hunt, Kaufmann & Reynolds 2006

Interfaces between interactive provers

Transferring results:

- hol90 → Nuprl: Howe and Felty 1997
- ACL2 → hol90: Staples 1999
- ACL2 → HOL4: Gordon, Hunt, Kaufmann & Reynolds 2006

Transferring proofs:

- hol90 → Coq: Denney 2000
- hol90 → NuPRL: Naumov, Stehr and Meseguer 2001
- HOL4 → Isabelle/HOL: Skalberg 2006
- HOL Light → Isabelle/HOL: Obua 2006
- Isabelle/HOL → HOL Light: McLaughlin 2006
- HOL Light → Coq: Keller 2009

More comprehensive sharing

There are at least two major projects that allow sharing between HOL-like systems

- OpenTheory (Hurd) — a general framework designed to support the transfer of theorems and proofs between HOL family provers
- HOL Zero (Adams) — simple and transparent version of HOL designed as a vehicle for proof import and checking with importers from other HOLs.

More comprehensive sharing

There are at least two major projects that allow sharing between HOL-like systems

- OpenTheory (Hurd) — a general framework designed to support the transfer of theorems and proofs between HOL family provers
- HOL Zero (Adams) — simple and transparent version of HOL designed as a vehicle for proof import and checking with importers from other HOLs.

Even more in the spirit of the original QED vision is the Logosphere project, which uses the Twelf logical framework as the common 'metalogic':
`http://www.logosphere.org`