The QED Manifesto*

May 15, 1994

The development of mathematics toward greater precision has led, as is well known, to the formalization of large tracts of it, so that one can prove any theorem using nothing but a few mechanical rules.

– K. Gödel

If civilization continues to advance, in the next two thousand years the overwhelming novelty in human thought will be the dominance of mathematical understanding.

– A. N. Whitehead

1 What Is the QED Project and Why Is It Important?

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.

The QED project will be a major scientific undertaking requiring the cooperation and effort of hundreds of deep mathematical minds, considerable ingenuity by many computer scientists, and broad support and leadership from research agencies. In the interest of enlisting a wide community of collaborators and supporters, we now offer reasons that the QED project should be undertaken.

First, the increase of mathematical knowledge during the last two hundred years has made the knowledge, let alone understanding, of all, or even of the most important, mathematical results something beyond the capacity of any human. For example, few mathematicians, if any, will ever understand the entirety of the recently settled structure of simple finite groups or the proof of the four color theorem. Remarkably, however, the creation of mathematical logic and the advance of computing technology have also provided the means for building a computing system that represents all important mathematical knowledge in an entirely rigorous and mechanically usable fashion. The QED system we imagine will provide a means by which mathematicians and scientists can scan the entirety of mathematical knowledge for relevant results and, using tools of the QED system, build upon such results with reliability and confidence but without the need for minute comprehension of the details or even the ultimate foundations of the parts of the system upon which they build. Note that the approach will almost surely be an incremental one: the most important and applicable results will likely become available before the more obscure and purely theoretical ones are tackled, thus leading to a useful system in the relatively near term.

Second, the development of high technology is an endeavor of fabulously increasing mathematical complexity. The internal documentation of the next generation of microprocessor chips may run, we have heard, to thousands of pages. The specification of a major new industrial system, such as a fly-by-wire airliner or an autonomous undersea mining operation, is likely to be even an order of magnitude greater in complexity, not the least reason being that such a system would perhaps include dozens of microprocessors. We believe that an industrial designer will be able to take parts of the QED system and use them to build reliable formal mathematical models of not only a new industrial system but even the interaction of that system with a formalization of the external world. We believe that such large mathematical models will provide a key principle for the construction of systems substantially more

*A version of this appeared as 'The QED Manifesto' in *Automated Deduction – CADE 12*, Springer-Verlag, Lecture Notes in Artificial Intelligence, Vol. 814, pp. 238–251, 1994.

Authorship and copyright information for this document may be found at the end.

complex than those of today, with no loss but rather an increase in reliability. As such models become increasingly complex, it will be a major benefit to have them available in stable, rigorous, public form for use by many. The QED system will be a key component of systems for verifying and even synthesizing computing systems, both hardware and software.

The third motivation for the QED project is education. Nothing is more important than mathematics education to the creation of infrastructure for technology-based economic growth. The development of mathematical ability is notoriously dependent upon 'doing' rather than upon 'being told' or 'remembering'. The QED system will provide, via such techniques as interactive proof checking algorithms and an endless variety of mathematical results at all levels, an opportunity for the one-on-one presenting, checking, and debugging of mathematical technique, which it is so expensive to provide by the method of one trained mathematician in dialogue with one student. QED can provide an engaging and non-threatening framework for the carrying out of proofs by students, in the same spirit as a long-standing program of Suppes at Stanford for example. Students will be able to get a deeper understanding of mathematics by seeing better the role that lemmas play in proofs and by seeing which kinds of manipulations are valid in which kinds of structures. Today few students get a grasp of mathematics at a detailed level, but via experimentation with a computerized laboratory, that number will increase. In fact, students can be used (eagerly, we think) to contribute to the development of the body of definitions and proved theorems in QED. Let also us make the observation that the relationship of QED to education may be seen in the following broad context: with increasing technology available, governments will look not only to cut costs of education but will increasingly turn to make education and its delivery more cost-effective and beneficial for the state and the individual.

Fourth, although it is not a practical motivation, nevertheless perhaps the foremost motivation for the QED project is cultural. Mathematics is arguably the foremost creation of the human mind. The QED system will be an object of significant cultural character, demonstrably and physically expressing the staggering depth and power of mathematics. Like the great pyramids, the effort required (especially early on) may be great; but the rewards can be even more staggering than this effort. Mathematics is one of the most basic things that unites all people, and helps illuminate some of the most fundamental truths of nature, even of being itself. In the last one hundred years, many traditional cultural values of our civilization have taken a severe beating, and the advance of science has received no small blame for this beating. The QED system will provide a beautiful and compelling monument to the fundamental reality of truth. It will thus provide some antidote to the degenerative effects of cultural relativism and nihilism. In providing motivations for things, one runs the danger of an infinite regression. In the end, we take some things as inherently valuable in themselves. We believe that the construction, use, and even contemplation of the QED system will be one of these, over and above the practical values of such a system. In support of this line of thought, let us cite Aristotle, the Philosopher, the Father of Logic, 'That which is proper to each thing is by nature best and most pleasant for each thing; for man, therefore, the life according to reason is best and pleasantest, since reason more than anything else is man.' We speculate that this cultural motivation may be the foremost motivation for the QED project. Sheer aesthetic beauty is a major, perhaps the major, force in the motivation of mathematicians, so it may be that such a cultural, aesthetic motivation will be the key motivation inciting mathematicians to participate.

Fifth, the QED system may help preserve mathematics from corruption. We must remember that mathematics essentially disappeared from Western civilization once, during the dark ages. Could it happen again? We must also remember how unprecedented in the history of mathematics is the clarity, even perfection, that developed in this century in regard to the idea of formal proof, and the foundation of essentially the entirety of known mathematics upon set theory. One can easily imagine corrupting forces that could undermine these achievements. For example, one might suspect that there is already a trend towards believing some recent 'theorems' in physics because they offer some predictive power rather than that they have any meaning, much less rigorous proof, with a possible erosion in established standards of rigor. The QED system could offer an antidote to any such tendency. The standard, impartial answer to the question 'Has it been proved?' could become 'Has it been checked by the QED system?' Such a mechanical proof checker could provide answers immune to pressures of emotion, fashion, and politics.

Sixth, the 'noise level' of published mathematics is too high. It has been estimated that something between 50 and 100 thousand mathematical papers are published per year. Nobody knows for sure how many contain errors or how many are repetitions, but some pessimists claim the number of both is high. QED can help to reduce the level of noise, both by helping to find errors and by helping to support computer searches for duplication.

Seventh, QED can help to make mathematics more coherent. There are similar techniques used in various fields of mathematics, a fact that category theory has exploited very well. It is quite natural for formalizers to generalize definitions and propositions because it can make their work much easier.

Eighth, by its insistence upon formalization, the QED project will add to the body of explicitly formulated mathematics. There is mathematical knowledge that is neither taught in classes nor published in monographs. It is below what mathematicians call 'folklore,' which is explicitly formulated. Let us call this lower level of unformulated knowledge 'mathlore'. In formalization efforts, we must formalize everything, and that includes mathlore lemmas.

Ninth, the QED project will help improve the low level of self-consciousness in mathematics. Good mathematicians understand trends and connections in their field. The QED project will enable mathematicians to analyze, perhaps statistically, the whole structure of the mathematics, to discover new trends, to forecast developments and so on.

2 Some Objections to the Idea of the QED Project and Some Responses

The peculiarity of the evidence of mathematical truths is that all the argument is on one side. There are no objections, and no answer to objections.

– J. S. Mill

Objection 1: *Paradoxes, Incompatible Logics, etc. Anyone familiar with the variety of mathematical paradoxes, controversies, and incompatible logics of the last hundred years will realize that it is a myth that there is certainty in mathematics. There is no fundamentally justifiable view of mathematics which has wide support, and no widely agreeable logic upon which such an edifice as QED could be founded.*

First Reply to Objection 1: Although there are a variety of logics, there is little doubt that one can describe all important logics within an elementary logic, such as primitive recursive arithmetic, about which there is no doubt, and within which one can reliably check proofs presented in the more controversial logics. We plan to build the QED system upon such a 'root logic', as we discuss below extensively. But the QED system is to be fundamentally unbiased as to the logics used in proofs. Or if there is to be a bias, it is to be a bias towards universal agreement. Proofs in all varieties of classical, constructive, and intuitionist logic will be found rigorously presented in the QED system – with sharing of proofs between logics where justified by metatheorems. For example, Goedel showed how to map theorems in classical number theory into intuitionist number theory, and E. Bishop showed how to develop much of modern mathematics in a way that is simultaneously constructive and classical. A mathematical logic may be regarded as being very much like a model of the world – one can often profit from using a model even if one ultimately chooses an alternative model because it is more suited to one's purposes. Furthermore, merely because some logic is so overly strong as to be ultimately found inconsistent or so weak as to ultimately fail to be able to express all that one hopes, one can nevertheless often transfer almost all of the technique developed in one logic to a subsequent, better logic.

Second Reply to Objection 1. These are controversies in the Philosophy of Mathematics. Who cares? The overwhelming majority of contemporary mathematicians believe that there are no doubts about what it means for a proof to be correct, and they agree on a vast common mathematical basis, much stronger than ZFC. If we do not get the mathematicians involved, the QED project will fail as well. But to get mathematicians involved, we have to find out how to talk to them.

Objection 2. *Intellectual property problems. Such an enterprise as QED is doomed because as soon as it is even slightly successful, it will be so swamped by lawyers with issues of ownership, copyright, trade secrecy, and patent law that the necessary wide cooperation of hundreds of mathematicians, computer scientists, research agencies, and institutions will become impossible.*

Reply to Objection 2. In full cognizance of the dangers of this objection, we put forward as a fundamental and initial principle that the entirety of the QED system is to be in the international public domain, so that all can freely benefit from it, and thus be inspired to contribute to its further development.

Objection 3. *Too much mathematics. Mathematics is now so large that the hope of incorporating all of mathematics into a system is utterly humanly impossible, especially since new mathematics is generated faster than it can be entered into any system.*

Reply to Objection 3. While it is certainly the case that we imagine anyone being free to add, in a mechanically checked, rigorous fashion, any sort of new mathematics to the QED system, it seems that as a first good objective, we should pursue checking 'named' theorems and algorithms, the sort of things that are commonly taught in universities, or cited as important in current mathematics and applications of mathematics.

Objection 4. *Mechanically checked formality is impossible. There is no evidence that extremely hard proofs can be put into formal form in less than some utterly ridiculous amount of work.*

Reply to Objection 4. Based upon discussions with numerous workers in automated reasoning, it is our view that using current proof-checking technology, we can, using a variety of systems and expert users of those systems, check mathematics at within a factor of ten, often much better, of the time it takes a skilled mathematician to write down a proof at the level of an advanced undergraduate textbook. QED will support proof checking at the speeds and efficiencies of contemporary proof-checking systems. In fact, we see one of the benefits of the QED project as being a demonstration of the viability of mechanically-assisted (-enforced) proof-checking.

Objection 5. *If QED were feasible, it would have already been underway several decades ago.*

Reply to Objection 5. Many of the most well-known projects related to QED were commenced in an era in which computing was exorbitantly expensive and computer communication between geographically remote groups was not possible. Now most secretaries have more computing power than was available to most entire QED-related projects at their inception, and rapid communication between most mathematics and computer science departments through email, telnet, and ftp has become almost universal. It also now seems unlikely that any one small research group can, alone, make a major dent in the goal of incorporating all of mathematics into a single system, but at the same time technology has made widespread collaboration entirely feasible, and the time seems ripe for a larger scale, collaborative effort. It is also worth adding that research agencies may now be in a better position to recognize the Babel of incompatible reasoning systems and symbolic computation systems that have evolved from a plethora of small projects without much attention to collaboration. Then perhaps they can work towards encouraging collaboration, to minimize the lack of interoperability due to diversity of theorem-statement languages, proof languages, programming languages, computing platforms, quality, and so on.

Objection 6. *QED is too expensive.*

Reply to Objection 6. While this objection requires careful study at some point, we note that simply concentrating the efforts of some currently-funded projects could go a long way towards getting QED off the ground. Moreover, as noted above, students could contribute to the project as an integrated part of their studies once the framework is established, presumably at little or no cost. We can imagine a number of professionals contributing as well. In particular, there is currently a large body of tenured or retired mathematicians who have little inclination for advanced research, and we believe that some of these could be inspired to contribute to this project. It may be a good idea to have a QED governing board to recognize contributions.

Objection 7. *Good mathematicians will never agree to work with formal systems because they are syntactically so constricting as to be inconsistent with creativity.*

Reply to Objection 7. The written body of formal logic rightly repulses most mathematical readers. Whitehead and Russell's Principia Mathematica did not establish mathematics in a notation that others happily adopted. The traditional definition of formal logics is in a form that no one can stand to use in practice, e.g., with function symbols named f_1, f_2, f_3, ... The absence of definitional principles for almost all formal logics is an indication that from the beginning, formal logics became something to be studied (for properties such as completeness) rather than to be used by humans, the practical visions of Leibniz and Frege notwithstanding. The developers of proof checking and theorem-proving systems have done little towards making their syntax tolerable to mathematicians. Yet, on this matter of syntax, there is room for the greatest hope. Although the subject of mechanical theorem-proving in general is beset with intractable or unsolvable problems, a vastly improved computer-human interface for mathematics is something easily within the grasp of current computer theory and technology. The work of Knuth on TEX and the widespread adoption of TEX by mathematicians and mathematics journals demonstrates that it is no problem for computers to deal with any known mathematical notation. Certainly, there is hard work to be done on this problem, but it is also certainly within the capacity of computer science to arrange for any rigorously definable syntax to be something that can be conveniently entered into computers, translated automatically into a suitable internal notation for formal purposes, and later reproduced in a form pleasant to humans. It is certainly feasible to arrange for the users of the QED system to be able to shift their syntax as often as they please to any new syntax, provided only that it is clear and unambiguous. Perhaps the major obstacle here is simply the current scientific reward system: precisely because new syntaxes, new parsers, and new formatters are so easy to design, little or no credit (research, academic, or financial) is currently available for working on this topic. Let us add that we need take no position on the question whether mathematicians can or should profit from the use of formal notations in the discovery of serious, deep mathematics. The QED system will be mainly useful in the final stages of proof reporting, similar to writing proofs up in journals, and perhaps possibly never in the discovery of new insights associated with deep results.

Objection 8. *The QED system will be so large that it is inevitable that there will be mistakes in its structure, and the QED system will, therefore, be unreliable.*

Reply to Objection 8. There is no doubt considerable room for error in the construction of the QED system, as in any human enterprise. A key motivation in Babbage's development of the computer was his objective of producing mathematical tables that had fewer errors than those produced by hand methods, an objective that has certainly been achieved. It is our experience that even with the primitive proof checking systems of today, errors made by humans are frequently found by the use of such tools, errors that would perhaps not otherwise be caught. The standard of success or failure of the QED project will not be whether it helps us to reach the kingdom of perfection, an unobtainable goal, but whether it permits us to construct proofs substantially more accurately than we can with current hand methods. In defense of the QED vision, let us assert that we believe that room for error can be radically reduced by (a) expressing the full foundation of the QED system in a few pages of mathematics and (b) supporting the development of essentially independent implementations for the basic checker. It goes without saying that in the development of any particular subfield of mathematics, errors in the statements of definitions and other axioms are possible. Agreement by experts in each mathematical subfield that the definitions are 'right' will be a necessary part of establishing confidence that mechanically checked theorems establish what is intended. There is no mechanical method for guaranteeing that a logical formula says what a user intuitively means.

Objection 9. *The cooperation of mathematicians is essential to building the QED edifice of proofs. However, because it is likely to remain very tedious to prove theorems formally with mechanical proof checkers for the foreeable future, mathematicians will have no incentive to help.*

Reply to Objection 9. To be developed, QED does not need to attract the support of all or most mathematicians. If only a tenth of one percent of mathematicians could be attracted, that will probably be sufficient. And in compensation for the extra work currently associated with entering formal mathematics in proof checking systems, we can point out that some mathematicians may find the following benefit sufficiently compensatory: in formally expressing mathematics, one's own thoughts are often sharply clarified. One often achieves an appreciation for subtle points in proofs that one might otherwise skim over or skip. And the sheer joy of getting all the details of a hard theorem 'exactly right', because formalized and machine checked, is great for many individuals. So we conjecture that enough mathematicians will be attracted to the endeavor provided it can be sufficiently organized to have a real chance of success.

Objection 10. *The QED project represents an unreasonable diversion of resources to the* *pursuit of the checking of ordinary mathematics when there is so much profitably to be done in support of the verification of hardware and software.*

Reply to Objection 10. Current efforts in formal, mechanical hardware and software verification are exceptionally introspective, focusing upon internal matters such as compilers, operating systems, networks, multipliers, and busses. From a mathematical point of view, essentially all these verifications fall into a tiny, minor corner of elementary number theory. But eventually, verification must reach out to consider the intended effect of computing systems upon the external, continuous world with which they interact. If one attempts to try to verify the use of a DSP chip for such potentially safety critical applications as telecommunications, robot vision, speech synthesis, or cat scanning, one immediately sees the need for such basic engineering mathematics as Fourier transforms, not something at which existing verification systems are yet much good. By including the rigorous development of the mathematics used in engineering, the QED project will make a crucial contribution to the advance of the verification of computing systems.

Objection 11. *The notion that interesting mathematics can ever, in practice, be formally checked is a fantasy. Whitehead and Russell spent hundreds of pages to prove something as trivial as that* 0 *is not* 1*. The notion that computing systems can be verified is another fantasy, based upon the misconception that mathematical proof can guarantee properties of physical devices.*

Reply to Objection 11. That many interesting, well-known results in mathematics can be checked by machine is manifest to those who take the trouble to read the literature. One can mention merely as examples of mathematics mechanically checked from first principles: Landau's book on the foundations of analysis, Girard's paradox, Rolle's theorem, both Banach's and Knaster's fixed point theorems, the mean value theorem for derivatives and integrals over Banach-space valued functions, the fundamental counting theorem for groups, the Schroeder-Bernstein theorem, the Picard-Lindelof theorem for the existence of ODEs, Wilson's theorem, Fermat's little theorem, the law of quadratic reciprocity, Ramsey's theorem, Goedel's incompleteness theorem, and the Church-Rosser theorem. That it is possible to verify mechanically a simple, general purpose microprocessor from the level of gates and registers up through an application, via a verified compiler, has been demonstrated. So there is no argument against proof-checking or mechanical verification in principle, only an ongoing and important engineering debate about cost-effectiveness. The noisy verification debate is largely a comedy of misunderstanding. In reaction to a perceived sanctimony of some verification enthusiasts, some opponents impute to all enthusiasts grandiose claims that complete satisfaction with a computing product can be established by mathematical means. But any verification enthusiast ought to admit that, at best, verification establishes a consistency between one mathematical theory and another, e.g., between a formal specification of intended behavior of a system and a formal representation of an implementation, say in terms of gates and memory. Mathematical proof can establish neither that a specification is what any user 'really wants' nor that a description of gates and memory corresponds to physical reality. So whether the results of a computation will be pleasing to or good for humans is something that cannot be formally stated, much less proved.

Objection 12. *The QED Manifesto is too long. Its length will interfere with the establishment of the project by driving away potential supporters and contributors.*

Reply to objection 12. Objection 12 is largely correct. For an initial reading, it is suggested that sections 4 and 5 below be skipped. On the other hand, we believe that there is real value in recording the many views on this subject, even views that are clearly refutable.

3 Some Background, Being a Critique of Current Related Efforts

Although the root of logic is the same for all, the 'hoi polloi' live as though they have a private understanding.

– Heraclitus

In some sense project QED is already underway, via a very diverse collection of projects. Unfortunately, progress seems greatly slowed by duplication of effort and by incompatibilities. If the many people already involved in work related to QED had begun cooperation twenty-five years ago in pursuing the construction of a single system (or federation of subsystems) incorporating the work of hundreds of scientists, a substantial part of the system, including at least all of undergraduate and much of first year graduate mathematics and computer science, could already have been incorporated into the QED system by now. We offer as evidence the nontrivial fragments of that body of theorems that has been successfully completed by existing proof-checking systems.

The idea of QED is perhaps 300 years old, but one can imagine tracing it back even 2500 years. We can agree that many groups and individuals have made substantial progress on parts of this project, yet we can ask the question, is there today any project underway which can be reasonably expected to serve as the basis for QED? We believe not, we are afraid not, though we would be delighted to join any such project already underway. One of the reasons that we do not believe there is any such project underway is that we think that there exist a few basic, unsolved technical problems, which we discuss below. A second reason is that few researchers are interested in doing the hard work of checking proofs – probably due to an absence of belief that much of the entire QED edifice will ever be constructed. Another reason is that we are familiar with many automated reasoning projects but see very serious problems in many of them. Here are some of these problems.

1. *Too much code to be trusted.* There have been a number of automated reasoning systems that have checked many theorems of interest, but the amount of code in some of these impressive systems that must be correct if we are to have confidence in the proofs produced by these systems is vastly greater than the few pages of text that we wish to have as the foundation of QED.

2. *Too strong a logic.* There have been many good automated reasoning systems that 'wired in' such powerful rules of inference or such powerful axioms that their work is suspect to many of those who might be tempted to contribute to QED – those of an intuitionistic or constructivist bent.

3. *Too limited a logic.* Some projects have been developed upon intuitionistic or constructive lines, but seem unlikely, so far anyway, to support also the effective checking of theorems in classical mathematics. We regard this 'boot-strapping problem' – how to get, rigorously, from checking theorems in a weak logic to theorems in a powerful classical logic, in an effective way – to be a key unsolved technical obstacle to QED. We discuss it further below.

4. *Too unintelligible a logic.* Some people have attempted to start projects on a basis that is extremely obscure, at least when observed by most of the community. We believe that if the initial, base, root logic is not widely known, understood, and accepted, there will never be much enthusiasm for QED, and hence it will never get off the ground. It will take the cooperation of many, many people to build the QED system.

5. *Too unnatural a syntax.* Just as QED must support a variety of logics, so too must it support a variety of syntaxes, enough to make most groups of mathematicians happy when they read theorems they are looking for. It is unreasonable to expect mathematicians to have to use some computer oriented or otherwise extremely simplified syntax when concentrating on deep mathematical thoughts. Of course, a rigorous development of the syntaxes will be essential, and it will be a burden on human readers using the QED proof tree to 'know' not only the logical theory in which any theorem or procedure they are reading is written but also to know the syntax being used.

6. *Parochialism.* There are many projects that have started over from scratch rather than building upon the work of others, for reasons of remoteness, ignorance of previous work, personalities, unavailability of code due to intellectual property problems, and issues of grants and publications. We are extremely sensitive to the fact that the issue of credit for scientific work in a large scale project such as this can be a main reason for the failure of the QED project. But we can be hopeful that if a sufficient number of scientists unite in supporting the QED project, then partial contributions to QED's advancement will be seen in a very positive light in comparison to efforts to start all over from scratch.

7. *Too little extensibility.* In 20 years there have been perhaps a dozen major proof-checking projects, each representing an

enormous amount of activity, but which have 'plateaued out' or even evaporated. It seems that when the original authors of these systems cease actively working on their systems, the systems tend to die. Perhaps this problem stems from the fact that insufficient analysis was given to the basic problems of the root logic. Without a sufficient amount of extensibility, everyone so far seems to have reached a point in which checking new proofs is too much work to do by machine, even though one knows that it is relatively easy for mathematicians to keep making progress by hand. The reason, we suspect, is that mathematicians are using some reflection principles or layers of logics in ways not yet fully understood, or at least not implemented. Mathematicians great contribution has been the continual re-evaluating, re-conceptualizing, connecting, extending and, in cases, discarding of theorems and areas. So each generation stands on the shoulders of the giants before, as if they had always been there. We are far from being able to represent mechanically such evolutionary mathematical processes. Existing mathematical logics are typically as 'static' as possible, often not even permitting the addition of new definitions! Important work in logic needs to be done to design logics more adaptable to extension and evolution.

8. *Too little heuristic search support.* While it is in principle possible to generate entries in the QED system entirely by hand, it seems extremely likely that some sort of automated tools will be necessary, including tools that do lots of search and use lots of heuristics or strategies to control search. Some systems which have completely eschewed such search and heuristic techniques might have gotten much further in checking interesting theorems through such techniques.

9. *Too little care for rigor.* It is notoriously easy to find 'bugs' in algorithms for symbolic computation. To make matters worse, these errors are often regarded as of no significance by their authors, who plead that the result returned is true 'except on a set of measure zero', without explicitly naming the set involved. The careful determination, nay, even proof, of precisely which conditions under which a result is true is essential for building the structure of mathematics so that one can depend on it. The QED system will support the development of symbolic algebra programs in which formal proofs of correctness of derivations are provided, along with the precise statement of conditions under which the results are true.

10. *Complete absence of inter-operability.* One safe generalization about current automated reasoning or symbolic computation systems is that it is always somewhere between impossible and extremely difficult to use any two of them together reliably and mechanically. It seems almost essential to the inception of any major project in this area to choose a logic and a syntax that is original, i.e., incompatible with other tools. One major exception to this generalization is the base syntax and logic for resolution systems. Here, standard problem sets have been circulated for years. But even for such resolution systems there is no standard syntax for entering problems involving such fundamental mathematical constructs as induction schemas or set-builder notation.

11. *Too little attention paid to ease of use.* The ease of use of automated reasoning systems is perhaps lower than for any other type of computing system available! In general, while anyone can use a word processor, almost no one but an expert can use a proof checker to check a difficult theorem. Perhaps this can be explained by the fact that the designers of such systems have had to put so much of their energies and attention into rigor, that they simply did not have enough energy left for good interface design.

4 The Relationship of QED to Artificial Intelligence (AI) and to Automated Reasoning (AR)

Project QED is largely independent of the question of the possibility or utility of artificial intelligence or automated reasoning. To the extent that mechanical aids of any kind can be used to help construct (or shorten) entries in the QED system, we can be appreciative of such aids, even if the aids use techniques that are from the realms of artificial intelligence, assuming of course that what the aids suggest doing is verifiably correct. A key fact is that it will not matter, from the viewpoint of soundness, whether proofs were added to the QED system by humans, dumb programs, smart programs or some combination thereof. All of the QED system will be checkable by a simple program, from first principles. The QED system will focus on what is known in mathematics, both theorems and techniques, rather than upon the problems of discovering new mathematics.

It is the view of some of us that many people who could have easily contributed to project QED have been distracted away by the enticing lure of AI or AR. It can be agreed that the grand visions of AI or AR are much more interesting than a completed QED system while still believing that there is great aesthetic, philosophical, scientific, educational, and technological value in the construction of the QED system, regardless of whether its construction is or is not largely done 'by hand' or largely automatically.

5 The Root Logic – Some Technical Details

> *Method consists entirely in the order and disposition of the objects towards which our mental vision must be directed if we would find out any truth. We shall comply with it exactly if we reduce involved and obscure propositions step by step to those that are simpler, and then starting with the intuitive apprehension of all those that are absolutely simple, attempt to ascend to the knowledge of all others by precisely similar steps.*
>
> – R. Descartes

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. As a model for brevity and clarity, we can refer the reader to Goedel's presentation, in about two pages, of high-order logic with number theory and set theory, at the beginning of his famous paper on undecidable questions.

The reason that we emphasize succinctness in the description of the logic is that we hope that there will be many separate implementations of a proof checker for this 'root logic' and that each of these implementations can check the correctness of the entire QED system. In the end, it will be the 'social process' of mathematical agreement that will lead to confidence in the implementations of these proof-checkers for the root logic of the QED system, and multiple implementations of a succinct logic will greatly increase the chance this social process will occur.

It is crucial that a 'root logic' be a logic that is agreeable to all practicing mathematicians. 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. It has also been further developed by Goodstein. In PRA one finds (a) an absence of explicit quantification, (b) an ability to define primitive recursive functions, (c) a few rules for handling equality, e.g., substitution of equals for equals, (d) a rule of instantiation, and (e) a simple induction principle. One reason for taking such a logic as the root logic is that it is doubtful that Metamathematics can be developed in a weaker logic. In any root logic one needs to be able to define, inductively, an infinite collection of terms and, inductively, an infinite collection of theorems, using in the definition of 'theorem' such primitive recursive concepts as substitution. Thus PRA has the bare minimum power we would need to 'get off the ground'. Yet we think it suffices even for checking theorems in classical set theory, in a sense we describe below. The logic FS0, conservative over PRA, but with sets and quantifiers, has been proposed by Feferman as a vehicle more congenial than PRA for studying logics.

It is probably the case that the syntax of resolution theorem-proving is the most widely used and most easily understood logic in the history of work on mechanical theorem-proving and proof checking, and thus perhaps a resolution-like logic could serve as a natural choice for a root logic. Some may object on the grounds that resolution, being based upon classical first order logic, 'wires in' the law of the excluded middle, and therefore is objectionable to constructivists. In response to this objection, let us note that constructivists do not object to the law of the excluded middle in a free variable setting if all of the predicates and function symbols 'in sight' are recursively defined; for example, it is a constructive theorem that for all positive integers x and y, x divides y or x does not divide y. Thus we might imagine taking as a root logic resolution restricted to axioms describing recursive functions and hereditarily finite objects, such as the integers.

The lambda-calculus-based 'logical frameworks' work in Europe, in the de Bruijn tradition, is perhaps the most well developed potential root logic, with several substantial computer implementations which have already checked significant parts of mathematics. And already, many different logics have been represented in these logical frameworks. As a caution, we note that some may worry there is dangerously too much logical power in some of these versions of the typed lambda calculus. But such logical frameworks give rise to the hope that the root logic might be such that classical logic could simply be viewed as the extension of the root logic by a few higher-order axioms such as $\forall P\,(P \vee \neg P)$.

One possible argument in favor of adopting a root logic of power PRA is that its inductive power permits the proof of metatheorems, which will enable the QED system to check and then effectively use decision procedures. For example, the deduction theorem for first order logic is a theorem of FS0, something not provable in some logical framework systems, for want of induction.

Regardless of the strength or weakness of the root logic chosen, we believe that we can rigorously incorporate into the QED system any part of mathematics, including extremely non-constructive set theoretic arguments, because we can represent these arguments 'one level removed' as 'theorems' that a certain finite object is indeed a proof in a certain theory. For example, if we have in mind some high powered theorem, say, the independence of the continuum hypothesis, we can immediately think of a corresponding theorem of primitive recursive arithmetic that says, roughly, that some sequence of formulas is a proof in some suitable set theory, S1, of another theorem about some other set theory, where a, say, primitive recursive proof checker for S1 has been written in the root logic of QED. In practice, it will be highly advantageous if we make it appear that one isn't really proving a theorem of proof theory but rather is proving a theorem of group theory or topology or whatever.

Although many groups have built remarkable theorem-proving and proof checking systems, we believe that there is a need for some further scientific or computational advances to overcome some 'resource' problems in building a system that can hold all important mathematics. Simply stated, it appears that complete proofs of certain theorems that involve a lot of computation will require more disk space for their storage than could reasonably be expected to be available for the project. The most attractive solution to such a problem is the development of 'reflection' techniques that will permit one to use algorithms that have been rigorously incorporated within QED as part of the QED proof system.

Although we have spoken of a single root logic, we need to make clear that we do not want to fall into the trap of searching for a single, ideal logic. We can easily imagine that it will be possible to develop several different root logics each of which can be fully regarded to be 'a' foundation of QED, each of which is capable as acting as a basis for the other, and each of which has very short implementations which have been checked by the 'social process'. And each of which can be used to check the correctness of the entire QED system.

In any case, it is a highly desireable goal that a checker for the root logic can be easily written in common programming languages. The specification should be so unambiguous that many can easily implement it from its specification in a few pages of code, with total comprehension by a single person.

It has been argued that the idea of having multiple logics in addition to the root logic is a mistake that will result in too much complexity, and that it would be far more sensible to have a single logic in which proofs were clearly flagged with an indication of the assumptions used, so that a single logic could be enjoyed by people of both classical and constructive persuasions. Certainly such a single logic is desireable, but whether such a single logic can be developed is a serious question given that some famous constructive theorems (such as the continuity of all functions on the reals) are classical falsehoods.

It has been argued that the idea of searching for a single logic or a single computer system is inferior to the idea of developing translation mechanisms that would permit proof checking systems to exchange proofs with one another. If this were feasible, it would certainly permit an alternative, distributed approach to achieving the major QED objectives. However, the history of radical incompatibility of many proof checking systems does suggest that such translation mechanisms may be difficult to produce.

In seeking a root logic, it is clear that there will be many controversies that will be impossible to resolve to everyone's satisfaction. For example, there seems no hope of satisfying in a single logic those who insist upon a typed syntax and those who loathe typed syntax, preferring to do typing internally, e.g., with sets. There are also simple questions not yet resolved after centuries of thought, such as the semantics of a function applied outside its domain, e.g., division by zero.

6 What Is To Be Done?

> *The idea is to make a language such that everything we write in it is interpretable as correct mathematics ... This may include the writing of a vast mathematical encyclopedia, to which everybody (either a human or a machine) may contribute what he likes. The idea of a kind of formalized encyclopedia was already conceived and partly carried out by Peano around 1900, but that was still far from what we might call automatically readable.*
>
> – N. G. de Bruijn

Leadership. It seems certain that inviting deliberation by many interested parties at the planning stage is important not only to get the QED project off on a correct footing but also to encourage many to participate in the project. Until we can establish general agreement within a large, critical mass of scientists (including many distinguished mathematicians) that the QED project is probably worth doing, and until a basic 'manifesto' agreeable to them can be drafted, possibly using parts of this document as a starting point, it is not clear whether there will be any further progress on this project. Given the extraordinary scope of this project, it is also essential that research agency leadership be obtained. It is perhaps unlikely that any one agency would be willing to undertake the funding of the entirety of such a large project. So an agreement by many agencies to cooperate will probably be essential. The requirements for leadership, both by scientists and by research agencies, are so major that it is perhaps premature to speculate about what other things should be done, in what order. Nevertheless, we will speculate about a few issues.

What planning steps should be taken to start the QED project? An obvious first concern is to enumerate and describe in some detail the kinds of things that would be found in the QED system, including

- logics
- axioms
- definitions
- theorems (including an analysis of the major parts of mathematics)
- proofs
- proof-checkers
- decision procedures
- theorem-proving programs
- symbolic computation procedures
- modeling software
- simulation software
- tools for experimentation
- numerical analysis software
- graphical tools for viewing mathematics
- interface tools for using the QED system

Crucial to this initial high level organization effort is deciding what parts of mathematics will be represented, how that mathematics will be organized, and how it will be presented. It is conceivable that years of consideration of these points should precede implementation efforts. One can imagine that a re-organization of mathematics on the order of the scope of the Bourbaki project is necessary. One can imagine major projects in the development of formal 'higher-level' languages in which mathematics can be formally discussed and major projects devoted simply to writing the most important theorems, definitions, and proof sketches in such languages. Because different proofs of the same theorem can differ substantially in complexity, and because entering formal proofs into a proof checking system is very expensive, it is highly cost effective to consider many proofs of a theorem before setting out to verify one of them. It has been suggested by several people that a useful and relatively easy early step would be to assemble, in ftp-able form, a comprehensive survey of the parts of mathematics have been checked by various automated reasoning systems.

A second planning step would be to establish some 'milestones' or some priority list of objectives. For example, one could attempt to outline which parts of mathematics should be added to the system in what order. Simultaneously, an analysis of what sorts of cooperation and resources would be necessary to achieve the earlier goals should be performed.

A third planning step would be to accumulate the basic mathematical texts that are to be formalized. It is entirely possible that the QED project will greatly overlap with an effort to build an electronic library of mathematical information. It is not part of the idea of a library that the documents should be in any particular language or subjected to any sort of rigor check. But it would of great inherent value, and great value to the QED project, to have the important works of mathematics available in machine readable form and organized for ease of access.

A fourth planning step would be to attempt to achieve consensus about the statement of the most important definitions and theorems in mathematics. Until there is agreement on the formalization of the basic concepts and theorems of the important parts of mathematics, it will be hardly appropriate to begin the difficult task of building formal proofs of theorems. The formalization of statements is an extremely difficult and error-prone activity.

Although the scientific obstacles to building QED are formidable, the social, psychological, political, and economic obstacles seem much greater. In principle, we can imagine a vast collection of people successfully collaborating on such an effort. But the problems of actually getting such a collaboration to occur are possibly insurmountable. 'Why,' an individual researcher could well ask, 'should I risk my future by working on what will be but a small part of a vast undertaking? What sort of recognition will I receive for contributing to yet one more computing system?' These are good questions, and it is not clear what the answer is. To a major extent, status in mathematics and computing is a function of publications in major journals – status for research funding, status for tenure decisions, status for promotion. It is far from clear how contributing pieces to the QED system could provide a substitute for such signs of status. Perhaps here research agencies or even university faculties and administrators could be of assistance in establishing a new societal framework in which such cooperation was encouraged.

Even given the cooperation of all the necessary people and assuming good luck in overcoming scientific hurdles, there are many issues of a very difficult but somewhat mundane character involving: version control, distribution, and support. A system with hundreds of contributors will create management difficulties perhaps not even imaginable to the small groups of researchers who have worked in the past on parts of the QED idea.

It has been suggested about the low-level QED data files that they should be humanly readable and permit comments, and that the character set should be email-able.

It has been suggested that the QED system should include historical information. Although such information would obviously not be something that would be mechanically checkable, it could provide extremely valuable contextual information to those trying to learn mathematics from the system, just as the commentaries on Euclid make his Elements intelligible to the modern reader. Strenuous disputes over priority in all forms of discovery, including mathematics, are common, and therefore care must be taken that the QED system permit the presentation of all sides of such disputes.

It has been suggested that it would be best if QED focused initially on one part of mathematics, namely ring theory.

Authorship: This preliminary discussion of project QED (very tentative name) is an amalgam of many ideas that many people have had and for which perhaps no one alive today deserves much credit. We are deliberately avoiding any authorship or institutional affiliation at this early stage in the project (and may decide to do so forever) in the hope that many will want to join in the project as principals, even as originators (to the extent that anyone alive today could be thought to be an originator of this project). Some of those involved in the project would much rather that QED be completed than that they, as individuals, be lucky enough to partake significantly in the project, much less get any public credit for its completion. It may seem paranoid to avoid personalities, but we are inspired by the extraordinary cooperation achieved in the Bourbaki series in an atmosphere of anonymity.

To join an Internet electronic discussion group devoted to the QED project, send a message with the single line

```
subscribe qed
```

to `majordomo@mcs.anl.gov`. The line above should be the content of the message, not the subject line. The subject line is ignored. An archive of this discussion group is in the directory `/pub/qed/archive/` available by anonymous ftp from `info.mcs.anl.gov`.