Downloaded from rsta.royalsocietypublishing.org on April 22, 2012

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Highly complex proofs and implications of such proofs

Michael Aschbacher

Phil. Trans. R. Soc. A 2005 **363**, 2401-2406
doi: 10.1098/rsta.2005.1655

Email alerting service Receive free email alerts when new articles cite this article - sign up in the box at the top right-hand corner of the article or click **here**

To subscribe to *Phil. Trans. R. Soc. A* go to:
http://rsta.royalsocietypublishing.org/subscriptions

Downloaded from rsta.royalsocietypublishing.org on April 22, 2012

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A

Phil. Trans. R. Soc. A (2005) **363**, 2401–2406
doi:10.1098/rsta.2005.1655
Published online 9 September 2005

Highly complex proofs and implications of such proofs

By Michael Aschbacher

Department of Mathematics, California Institute of Technology, Pasadena, CA 91125, USA
(asch@its.caltech.edu)

Conventional wisdom says the ideal proof should be short, simple, and elegant. However there are now examples of very long, complicated proofs, and as mathematics continues to mature, more examples are likely to appear. Such proofs raise various issues. For example it is impossible to write out a very long and complicated argument without error, so is such a 'proof' really a proof? What conditions make complex proofs necessary, possible, and of interest? Is the mathematics involved in dealing with information rich problems qualitatively different from more traditional mathematics?

Keywords: complex; proof; simple group; classification

Conventional wisdom says the ideal mathematical proof should be short, simple and elegant. However, there are now examples of very long, complicated proofs, and as mathematics continues to mature, more examples are likely to appear.

I have some experience with one such effort: the Classification of the finite simple groups. I'm going to use the Classification theorem and its proof as a basis for discussion, but I'm not going to state the theorem or go into details about the proof. Rather I'll treat the Classification and its proof as a black box, in that I'll begin by listing some features of the theorem and its proof, and later use them to help illustrate some of the points I hope to make.

First, the proof of the Classification is very long and complicated. As a guess, the proof involves perhaps 10 000 pages in hundreds of papers, written by hundreds of mathematicians. It would be difficult to establish exactly which papers are actually a necessary part of the proof, and I know of no published outline. At least this last difficulty will be eliminated by a program in progress, whose aim is to carefully write down in one place a complete and somewhat simplified version of most of the proof. Still there has not been as much improvement and simplification of the original proof as one might expect.

Second, the theorem is very useful. One cannot do serious finite group theory without the Classification, and it has made possible numerous applications of finite group theory in other branches of mathematics. One can speculate that a proof of the complexity of the Classification would be unlikely to evolve in the absence of such strong incentives. One can also speculate that such theorems can only be proved via some kind of evolutionary process: the extent of the problem

One contribution of 13 to a Discussion Meeting Issue 'The nature of mathematical proof'.

© 2005 The Royal Society

Downloaded from rsta.royalsocietypublishing.org on April 22, 2012

and possible paths to a solution only become visible after a large amount of preliminary investigation and experimentation.

Third, at first glance the Classification is a prototypical classification theorem: It considers a class C of objects (in this case the class of finite simple groups), supplies a list L of objects in the class and proves that each member of C is isomorphic to exactly one member of L.

But also fourth, the collection L of examples is large, varied, and of great interest, and each member has a rich structure. The Classification does more than just show L and C are equal; its proof supplies a wealth of detailed information about the structure of members of L. Such information is a prerequisite for applying the Classification. Thus after a bit more thought, the Classification is more than just a 'classification theorem'.

Fifth, the proof is inductive and depends upon a good knowledge of the structure of members of L. That is to say one considers a minimal counter example to the Classification: an object G of minimal order subject to G in C but not in L. Then all proper simple 'sections' of G in C are in L, and most arguments are based on strong information about such sections, available in the inductive context.

As an aside, it is worth noting that there exists no theorem which says: Each sufficiently large member of C is in L. If we've made mistakes, so that the theorem is false and there is some H in $C - L$, then it might be possible to repair the theorem by adding H to L and making minor modifications to the inductive 'proof'. This would be true if the structure of H is much like that of the members of L. But if H has a very different structure, one could imagine that such a modification might not be possible.

Now I'd like to draw some implications from the example. I began with the observation that the ideal proof is short, simple, and elegant. The proof in our example has none of these desirable qualities. That hasn't stopped mathematicians from appealing to the theorem, but it does raise various questions.

First, because of the complexity of the proof and the absence of a definitive treatment in the literature, one can ask if the theorem has really been proved. After all, the probability of an error in the proof is one. Indeed, presumably any attempt to write down a proof of such a theorem must contain many mistakes. Human beings are not capable of writing up a 10 000 page argument which is entirely free of errors. Thus if we demand that our proofs be error free, then the Classification can't be proved via techniques currently available.

However in practice, mathematicians seem only to take this idealized notion of a proof as a model toward which to strive. The real standard would appear to be an argument which deals carefully with all fundamental difficulties, and which organizes and does due diligence to the small details, so that there are few gaps or minor errors, and those that exist can be filled in or repaired without much difficulty by the reader. I suspect most professional mathematicians feel that, after some (high) minimal standard of rigor has been met, it is more important that the proof convey understanding than that all formal details appear without error.

This suggests we should consider a bit more carefully the role 'proof' plays in mathematics. At Caltech, pure mathematics is part of the 'Division of Physics, Mathematics, and Astronomy'. This gives me a little insight into the difference between how mathematicians and physicists view the notion of 'proof'. For the physicist, the truth of a theory or hypothesis is established by testing it against

Downloaded from rsta.royalsocietypublishing.org on April 22, 2012

physical data. My sense is that most physicists feel proofs are nice, but not all that important.

On the other hand, for the mathematician, truth is established via proofs, since that portion of a particular mathematical universe visible via 'experiment' may be too small to be representative of the total universe. But the process of producing a proof does more: It leads to a deeper understanding of the mathematical universe the mathematician is considering.

Moreover, proofs and fields of mathematics evolve over time. The first proof of a theorem is usually relatively complicated and unpleasant. But if the result is sufficiently important, new approaches replace or refine the original proof, usually by embedding it in a more sophisticated conceptual context, until the theorem eventually comes to be viewed as an obvious corollary of a larger theoretical construct. Thus proofs are a means for establishing what is real and what is not, but also a vehicle for arriving at a deeper understanding of mathematical reality.

By concensus of the community of group theorists, the Classification has been accepted as a theorem for roughly 25 years, despite the fact that, for at least part of that period, gaps in the proof were known to exist. At this point in time, all known gaps have been filled. The most significant of these (involving the so-called 'quasithin groups') was only recently removed in the lengthy two volume work of Aschbacher and Smith. During the 25 years, the proof of the Classification has not evolved as much as one might expect. Some simplifications and conceptual improvements to certain parts of the argument have emerged, and there is a program in progress to write down the proof more carefully in one place. Dependence on computer aided proofs for the existence and uniqueness of the so-called sporadic groups has been almost entirely eliminated. But for the most part the proof still has the same shape and complexity.

To set the stage for one explanation of these facts, and to further explore why the proof of the Classification (and by extension other proofs) should be so complicated, I present a quote from the biologist John Hopfield talking about the core curriculum at Caltech:

> Physics was …often presented as the paradigm for how science should be done. The idea was that a science should require as little actual knowledge as possible, and that all conclusions should follow from a very small set of facts and equations… Biology is an information-rich subject. Complex structures and behaviors are intrinsic to (and the essence of) biology and other information rich sciences.
>
> *John Hopfield*

I believe the Classification is an example of mathematics coming to grips with a complex information rich problem using both Hopfield's physics paradigm and his biology paradigm. The hypothesis of the theorem is simple and easily understood by anyone who has taken a decent undergraduate course in abstract algebra. The conclusion also appears at first glance to be at least moderately simple. However, when one looks more closely, one finds that it takes some effort and sophistication to define many of the examples. Moreover, the utility of the theorem stems from two facts: First. it seems to be possible to reduce most questions about finite groups to questions about simple groups. Second, the explicit description of the groups on the list L supplied by very effective

Downloaded from rsta.royalsocietypublishing.org on April 22, 2012

representations of most of the groups, make it possible to obtain a vast amount of detailed information about the groups.

Fact one makes it possible to avoid the untenable complexity and relative lack of structure of the general finite group. The reduction from the general finite group to the finite simple group corresponds to a reduction from a universe with relatively little structure and much complexity (such as the universe of biology) to a universe with a lot of structure and manageable complexity. But for those who use the theorem, those changes are hidden in the proof.

However consumers must still grapple with the complexity inherent in the simple groups themselves. This is where fact two comes in. More and more in modern mathematics, particularly in problems in discrete mathematics coming from fields like information theory, computer science, or biology, one must deal with objects with little classical mathematical structure, but under hypotheses placing strong constraints on the objects which are difficult to exploit in the absence of structure. Many such problems can be translated into the domain of group theory, where suitable information about simple groups can be used to obtain a solution.

Further, I speculate that the Classification is itself an early example of this kind of result. *A priori* it is difficult to make use of the hypothesis that a group is simple: the assumption does not automatically supply a nice representation of the group. The variety of examples in L suggest this must be true. Instead, one must exploit detailed information about the members of L in the inductive setting of the minimal counter example, operating more in the paradigm of biology than in the paradigm of physics or classical mathematics. It is my sense that there is an overabundance of information in the problem, which makes possible many different proofs, depending on how one utilizes the information. Producing a good proof in such a situation may be less a result of a clever idea or a new, better point of view, than of optimal organization of a very large set of data, and good technique.

My guess is that we will begin to encounter many more such problems, theorems, and proofs in the near future. As a result we will need to re-examine what constitutes a proof, and what constitutes a good proof. Elegance and simplicity should remain important criteria in judging mathematics, but the applicability and consequences of a result are also important, and sometimes these criteria conflict. I believe that some fundamental theorems do not admit simple elegant treatments, and the proofs of such theorems may of necessity be long and complicated. Our standards of rigor and beauty must be sufficiently broad and realistic to allow us to accept and appreciate such results and their proofs. As mathematicians we will inevitably use such theorems when it is necessary in the practice our trade; our philosophy and aesthetics should reflect this reality.

This work was partially supported by NSF-0203417.

Discussion

P. H. A. Sneath (*Infection, Immunity and Inflammation, University of Leicester, UK*). In biology one must often make a large number of assumptions before one

Downloaded from rsta.royalsocietypublishing.org on April 22, 2012

can formulate a theorem, and then the proof may be very simple. The question is whether it is really a proof. To give an example from bacteriology, how does one identify a strain of the typhoid bacillus, *Salmonella typhi*, and prove the identity? In principle one collects many strains that have certainly come from cases of typhoid fever, and determines numerous properties of these accurately. One then sets up a model in which the species *S. typhi* can be likened to a swarm of bees in a multidimensional space. An unknown strain is identified as *S. typhi* if it lies within the swarm. But after making these and other assumptions (including that the variation is haphazard,—effectively ramdom,—and that the swarm is perhaps distributed multivariate normally—but not multivariate logistically) the proof is simple. One can obtain the probability that the unknown bacillus is a typhoid bacillus from the well-known properties of the normal distribution. Further, the results are robust; a few mistakes do not greatly damage the conclusions. But it is evident the prior assumptions are the critical factor, because one can scarcely check the identity by infecting a volunteer.

M. Aschbacher. Sneath gives an example where a biological process is modeled by a mathematical system. As I interpret it, he then asks: Is a proof of a theorem in the mathematical system, also a 'proof' of a 'theorem' about biology? It would seem to me that the notions of 'theorem' and 'proof' (at least as understood by mathematicians) are particular to mathematics. As Sneath suggests, the information the mathematical theorem gives about the biological problem, is only as good as the fit of the mathematical model to the original problem. Even if the fit is good, it is not clear to me that translations of theorems and proofs in the mathematical setting to the biological setting can be called 'theorems' and 'proofs' without straining the meaning of those words to the breaking point. On the other hand theorems in the mathematical setting do give biological information when the model is good.

A. Bundy (*School of Informatics, University of Edinburgh, UK*). How can we account for the unreasonable robustness of proofs? Naively, we might expect most errors in proofs to be fatal, but many are readily fixed. Why is this?

M. Aschbacher Some proofs are robust and others are not. I think mathematicians operate on at least two levels: the formal and the intuitive. Consider an area of mathematics where formal machinery is in place, which has been worked out fairly carefully and in detail, and in addition the intuition of the community of specialists in the area is in tune with that machinery. In such a situation, theorems advanced by capable members of the community are usually unlikely to have large, irreparable errors, or at least it is unlikely that such errors will not be discovered by the community. The intuition of the community (and the individual) will normally lead them to those places in the proof where serious errors are likely to occur. In such a situation the individual mathematician usually finds serious errors in his or her proof, before the proof sees the light of day, and the community identifies flawed mathematics before it gains wide acceptance. On the other hand, problems can arise when untested, unfamiliar machinery is applied, or when the community encounters a situation where counter intuitive phenomena are involved.

M. Atiyah (*School of Mathematics & Statistics, University of Edinburgh, UK*). An analogy has been made between evolutionary biology, in which complex

Downloaded from rsta.royalsocietypublishing.org on April 22, 2012

organisms emerged as a result of long random processes and natural selection, and complex mathematical problems such as the classification of finite simple groups; I think this is not a correct analogy. Finite simple groups did not emerge from some random choice of axiom systems, they were a product of the human mind, though reflecting the notion of symmetry in the natural world.

M. Aschbacher I think the analogy I'd draw is between the evolution of biological organisms and certain proofs. At some level, both the complex organism and the complex proof are examples of complex adaptive systems. True, proofs do not emerge entirely randomly. But for a long period of time, each individual mathematician working on his or her small part of the problem, almost certainly has no serious global strategy. As a group, the community's approach will be influenced by mathematical precedents, but in time new ideas will emerge which alter the accepted paradigms. Subgroups will concentrate on subproblems, and develop highly specialized mathematics to deal with their subproblem. Eventually enough structure emerges from the union of these specialties to suggest a global strategy. Finally a proof is achieved, but not a proof anyone could have foreseen when the process began. Moreover if different people had been involved, or if the same people had looked at things a bit differently, then a totally different proof might have resulted.

A. Ireland (*Department of Computer Sciences, Heriot-Watt University, UK*). To a large extent computer science is concerned with the systematic management of large and complex evolving artefacts (systems). Yesterday we heard from computer scientists and artificial intelligence practitioners on computer assisted reasoning. As a working mathematician, were there any ideas presented yesterday that you feel may assist you in managing the complexity of your evolving proofs?

M. Aschbacher I suspect that for the most part, one can't do much to manage complex proofs. In the case of the classification of the finite simple groups, at a fairly late stage in the game (about 1970), Danny Gorenstein began to speculate on a global strategy for a proof. In effect he called attention to certain subproblems, which appeared to be approachable, or almost approachable, and he put forward a somewhat vague vision of how to attack some of the subproblems, and how his various modules might be assembled into a proof. While his program was sometimes a bit far from what eventually emerged, in other instances he was fairly prescient. In any event, Gorenstein focused attention on the problem of classifying the finite simple groups, in the process making the effort more visible. He also gave it some structure and served as a clearing house for what had been done, and was being done. In short, Gorenstein managed the community of finite simple group theorists, and to a lesser extent, managed part of the development of the proof itself. But he was only able to accomplish even these limited goals at a fairly late stage in the game: The last 10 years of an effort which was reasonably intense for about 25 years, and in some sense went on for almost a century. That is to say, a long period of learning and experimentation was necessary before it was possible to develop a global idea of how a proof might proceed. Finally, these observations are really only about the sociology of the community searching for the proof, rather than about strategies and techniques for dealing with complex mathematics, beyond the obvious approach of partitioning a big problem into smaller pieces.