Proof by Computer and Proof by Human Transcript

Date: Monday, 15 April 2013 - 6:00PM

Location: Barnard's Inn Hall
Proof by Computer and Proof by Human

Tony Mann

For many pure mathematicians, proof is the heart of their subject. It gives mathematics its power. When we prove a mathematical fact, we are establishing the necessary truth of something which is independent of the constraints of the human mind, which transcends our physical existence. Beethoven’s symphonies, Michelangelo’s paintings are meaningful only in the context of human existence: they depend on the human senses. Newton and Einstein’s equations model the physical laws which happen to hold in our universe. But mathematical truths are true in every possible universe: even if there were no intelligent life, nineteen would still be a prime number. Or so many mathematicians believe (perhaps rather naively).

Here is John Dee writing in 1570:

A meruaylous newtralitie haue these thinges Mathematicall, ... In Mathematicall reasoninges, a probable Argument, is nothyng regarded: nor yet the testimony of sense, any whit credited: But onely a perfect demonstration, of truths certaine, necessary, and inuincible: vniuersally and necessarily concluded: is allowed as sufficient for an Argument exactly and purely Mathematical.

This talk is going to explore the use of computers in mathematical proof. We are going to begin by looking at a few examples of different kinds of proofs. These will be short, and while I hope to convey a little of the spirit of the mathematics, it doesn't matter if you don't follow the details. We'll then look at two famous cases where computers have been used to prove long-standing mathematical conjectures – the Four Colour Theorem and the Kepler Conjecture. We will end with some reflections on the present-day state of computer proof and on the future. I am drawing on two recent accounts from leading mathematicians: Sir Timothy Gowers’s London Mathematical Society popular lecture last year, and especially a wonderful survey account by Thomas Hales which appeared while I was preparing this lecture, without which tonight’s talk would have been very different.

So what is proof, and why is it so valued? A proof is an argument which demonstrates that a proposition must be true.

Here’s a problem: how many dots are in this hexagon, and how many would there be if there were n (rather than 7) dots on each side? We could count them, but there is an ingenious argument which shows us the answer. We can regard the image not as a two-dimensional hexagon but as a three-dimensional cube, of which we are seeing the top, front and left sides only. The portion of this cube which is hidden from us is a smaller cube of side n-1, so the number of dots is \( n^3 - (n-1)^3 \). Is this a rigorous proof? I’m really not quite sure!

For perhaps a sounder proof here’s a simple problem, famously solved by the great mathematician Gauss when he was a schoolboy. What is the sum of all the integers between 1 and n? I claim it’s \( \frac{1}{2} n(n+1) \), and I prove it as follows. I write out the sum as

\[ S = 1 + 2 + 3 + 4 + \ldots + (n-1) + n \]

But I can also write it in reverse:

\[ S = n + (n-1) + (n-2) + (n-3) + \ldots + 2 + 1 \]

Writing these together we have

\[ S = 1 + 2 + 3 + 4 + \ldots + (n-1) + n \]
\[ S = n + (n-1) + (n-2) + (n-3) + \ldots + 2 + 1 \]

We see that if we add each term in the first sum to the one directly below, we get \( n+1 \) each time.

\[
\begin{array}{cccccccc}
S & = & 1 & + & 2 & + & 3 & + & \ldots & + & (n-1) & + & n \\
S & = & n & + & (n-1) & + & (n-2) & + & (n-3) & + & \ldots & + & 2 & + & 1
\end{array}
\]

So if we add the two equations – since there are n terms in the sum – we get \( 2S = n(n+1) \), or \( S = \frac{1}{2} n(n+1) \) as I claimed. This is a direct proof, and it is conclusive - if someone follows the proof, they have to accept that the result is true.

Let’s prove the same result another way - by what I think of as the very wonderful method of mathematical induction. (My students, sadly, are often less enthusiastic!) A proof by induction has two parts. First - the
“basis” - one shows that the property one wishes to prove holds for (perhaps) the special case n=1. Then one shows that if the property holds for n=k, it also holds for n=k+1 - this is called the Inductive Step. Together these establish the case for all n greater than or equal to 1. Let’s show this by an example:

We want to show that the sum of the first n integers is \( \frac{1}{2} n(n+1) \). When n=1, the sum is 1 and \( \frac{1}{2} n(n+1) \) is \( \frac{1}{2} \cdot 1 \cdot 2 \) which is also 1, so the result we want to prove is true when n=1.

Suppose now the result is true when n=k, so that 1+2+3+…+k = \( \frac{1}{2} k(k+1) \). What happens when n is k+1? We want 1+2+3+…+k+(k+1) which by the inductive hypothesis is \( \frac{1}{2} k(k+1) + (k+1) \). A little algebra shows that this is \( \frac{1}{2} (k+1)(k+2) \), which is \( \frac{1}{2} n(n+1) \) when n=k+1. So we have established the inductive step: if our formula is true for n=k, it is also true for n=k+1.

I claim we have now established our result for all positive n. It is true for n=1. By the inductive step, since it is true for n=1, it is also true for n=2. Applying the inductive step again, since it is true for n=2 we can deduce that it is also true for n=3. And so on. For any integer r, we can show that the result holds by applying the inductive hypothesis repeatedly, starting from n=1, and after a finite number of steps we have established the result for n=r.

Proof by induction allows us to prove something for all positive integers through these two steps. The inductive hypothesis allows us to deal with infinitely many steps at the same time.

There are other forms of proof. Another which sometimes troubles my students is “Proof by contradiction” or “Reductio ad absurdum”. The idea here is that a true mathematical statement cannot lead to contradiction. So we see what happens if the result we want to prove is not true. If we can deduce that its non-truth leads to a contradiction, then we have shown that the result cannot not be true: that is, it must be true.

A classic example is Euclid’s famous proof that there are infinitely many prime numbers. (You may remember that a prime number is an integer greater than one which is divisible only by itself and one.) We show that if the proposition is not true, that is, there are only finitely many primes, then we have a contradiction. For if there are only finitely many primes, say 2, 3, 5, 7, up to p, the biggest prime, then we can calculate the product of all these primes – 2 times 3 times 5 times 7 times … up to times p – and add 1. This gives us

\[2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot p + 1\]

This number is one more than a multiple of 2, so it’s not divisible by 2. It also leaves a remainder of 1 when divided by 3, 5, 7, and every other prime number up to and including p, so it isn’t divisible by any of these. So it is either a prime number itself, or if not, its prime factors weren’t in our list of all the primes. In either case our complete list of all primes turns out not to have been complete. This is a contradiction, and the only resolution is that we could not, in fact, write down a finite list of all the primes: that is, we have proved that there are infinitely many prime numbers.

The tradition of proof goes back to perhaps the most famous book in the history of mathematics: Euclid’s Elements, written around 300BCE. We know almost nothing about Euclid - we don’t know how much of the Elements is his own work and how much is his presentation of older results - but the method of the Elements has defined the way pure mathematics has been practised for the last 2300 years. In short, Euclid states a number of definitions and common notions (for example, that things which equal the same thing also equal one another), and then five postulates, or axioms - self-evident statements that the reader will agree to be true. He then rigorously proves results about geometry using only these axioms and propositions which have already been proved from these axioms. That way the whole mathematical edifice is built on solid foundations. Every result must be true because it follows from the axioms and from things we have already established with absolute certainty.

Here is Euclid’s Proposition 1. It asserts that, given a straight line, it is possible to construct an equilateral triangle on it. We will prove this using only Euclid’s first four axioms. (I omit the fifth axiom - that is a different story, which Professor Flood has told well in one of his lectures this year.)

The first four axioms are:

Postulate 1: It is possible to draw a straight line from any point to any point

Postulate 2: It is possible to extend a finite straight line continuously in a straight line

Postulate 3: It is possible to draw a circle with any centre and any radius

Postulate 4: All right angles equal one another

To prove Proposition 1, we start with our given line AB. Using axiom 3, we describe a circle with centre A and radius AB. Using this axiom again, we describe another circle with centre B and radius AB. These circles meet at C: by axiom 1 we can draw the straight lines AC and BC. Now AC and BC are each equal to AB, since they are radii of the same circles, and by the common notion that things which equal the same thing also equal one another, we see that the triangle ABC has three sides of equal length. We have created the required equilateral
So a proof is a rigorous demonstration of the truth of a proposition. It is checkable. Each proof in Euclid’s elements can be checked by you or me: the truth of the propositions is certain and each of us can verify this for ourselves. One of the reasons proof is the “Gold standard” in mathematics is that it is checkable. Any of us can, in principle, satisfy ourselves that a published proof is correct. (In the case of Andrew Wiles’s proof of Fermat’s Last Theorem, that might take some time for most of us!)

Of course, it is possible to err in constructing a proof. Here’s a geometric proof of a statement that you might find slightly surprising (because it’s obviously not true!)

Proposition – there is no point inside a circle (this can be found in a rather nice little book published in 1959 by E.A. Maxwell, \textit{Fallacies in Mathematics}).

Proof: Take a circle with centre \(O\) and radius \(r\), and let \(P\) be any point inside the circle. We will prove that \(P\) actually must lie on the circumference.

Extend the line \(OP\) and take the point \(Q\) such that \(OP \cdot OQ = r^2\). Let the perpendicular bisector of \(PQ\) cut the circle at points \(U\) and \(V\), and let \(R\) be the midpoint of \(PQ\).

Now, \(OP = OR - RP\) and \(OQ = OR + RQ\) which is \(OR + RP\) since \(R\) is the midpoint of \(PQ\).

So \(OP \cdot OQ = (OR - RP) (OR + RP) = OR^2 - RP^2\)

We can now apply Pythagoras: \(OR^2 = OU^2 - RU^2\) and \(RP^2 = PU^2 - RU^2\), so

\[OP \cdot OQ = (OU^2 - RU^2) - (PU^2 - RU^2) = OU^2 - PU^2.\]

But \(OU^2 = r^2 = OP \cdot OQ\), since that was how we chose \(Q\). So we have

\[OU^2 = OU^2 - PU^2.\]

Whence we deduce \(PU = 0\), so \(P\) is the point \(U\) on the circumference of the circle. We have shown that there are no points in the circle.

The fallacy in this “proof” is left for the audience to identify. (In fact the “proof” does give us a genuinely interesting mathematical result, but not the one claimed.)

Perhaps, having seen this “proof”, you prefer proofs which don’t use diagrams. Here are two induction “proofs”.

\[\text{triangle on AB.}\]
Proposition: Any two integers are equal. (Maxwell)

For the proof, we use induction on the maximum of the two integers. If we have two integers of which the maximum is 1, then clearly they must both be one so the result holds. We will now show that, if it is true that any two integers of which the larger is k must be equal, then the result is also true for the case where the larger is k+1. For suppose we have integers m and n where the larger equals k+1. Then m-1 and n-1 are two integers of which the larger is k, so they must be equal by the inductive hypothesis. If n-1 = m-1 then certainly n = m. So we have proved the inductive step, and established the proposition.

Proposition: If we have a set of n horses, then every horse in the set is the same colour. (Halmos)

The proof is by induction on n, the number of horses in the set. If n=1, the set contains only one horse so it is certainly true that all horses in the set are the same colour. For the inductive step, suppose that the result is true for sets containing k horses. If we are given a set of k+1 horses, we can take the subset containing horses 1 to k: by the inductive hypothesis all are the same colour. We can also take the subset containing horses 2 to k+1; this is a set of k horses so they also are all the same colour. So horse k+1 is the same colour as horse k, which is the same colour as horses 1 to k-1, so they are all the same colour: we have proved the result.

None of these last three proofs is valid: it's instructive to find the (deliberate) errors! But, if they have made you pause for a moment, they have shown that it is possible to be misled by an apparent mathematical proof. These examples are frivolous, but there are plenty of cases of very good mathematicians producing erroneous proofs. The great Richard Feynman said "I have mathematically proven to myself so many things that aren't true." The most notorious example is Fermat's claimed but presumably incorrect proof of his Last Theorem. If Fermat did have a false proof, he was not alone: more than 1000 false proofs of Fermat's Last Theorem were published between 1908 and 1912!

You may feel that this has taken us a long way from the perfection of Euclid's rigour. But in fact there is a gap in Euclid's proof of his Proposition 1!

The proof assumed that two circles each of which passes through the centre of the other must intersect. This requires the Intermediate Value Theorem. This proof was eventually corrected by David Hilbert in 1899.

So human mathematicians are imperfect. We can be led astray: we make errors when creating and checking proofs. Computers carry out algorithms more accurately than people: can computers create and check proofs?

The first major public demonstration of a computer contribution to mathematical proof came when Kenneth Appel and Wolfgang Haken proved the Four Colour Theorem in 1976. This story has been well told by Professor Robin Wilson, in a Gresham College lecture you can watch online and in his book *Four Colours Suffice*, so I refer you to either of these excellent sources for a full account. The story is particularly instructive in the context of my lecture tonight.

The question is whether any map on the plane can be coloured with no more than four colours so that no two regions sharing a common boundary are the same colour (regions which meet only at a point can have the same colour).

Augustus de Morgan posed the question in 1852 and eventually in 1879 Alfred Bray Kempe proved that four colours are enough. Kempe's proof was ingenious, and introduced powerful new ideas: it isn't particularly difficult to follow, and had I longer I would show it to you. Unfortunately, however, it was irretrievably flawed, although it was over ten years before anyone noticed – Percy Heawood pointed out the error in 1889, by finding an example in which Kempe's method didn't work. This wasn't a counter-example to the theorem, but was sufficient to refute Kempe's proof.

I have to say that the error in Kempe's proof is subtle. When I was preparing to present the topic to my students, even knowing about the flaw, even with Heawood's counter-example in front of me, I still found the proof totally convincing!
So by the end of the nineteenth century the Four Colour Conjecture was open again, and despite attacks by a number of notable mathematicians, when I was a schoolboy it was one of the famous unsolved problems of mathematics. So Appel and Haken’s proof was exciting, but it was also controversial. They followed Kempe’s approach, which was in two parts. First one finds an “unavoidable set of configurations”, one of which must be present in any map. Then one shows that every one of this set is reducible, which means that if it is present in a map, that map can be coloured with only four colours. But whereas Kempe’s unavoidable set contained only two configurations, and could easily be checked by hand, Appel and Haken’s set contained almost 2000 configurations. The reducibility of each configuration was checked by a computer programme, not by hand. This involved over a thousand hours of computer time, and full checking by a human being was impossible.

The reaction from some mathematicians was not excitement at the solution to a longstanding problem, but rather horror! They said, “In my view such a solution does not belong to the mathematical sciences at all” or “God wouldn’t let the theorem be proved by a method as terrible as that!”. But mathematicians who hoped that the computer proof would be followed by an unaided human one have been disappointed: there is still no proof of the Four Colour Theorem that does not rely on computer calculations. While we can check the programmes, and check the hardware design of the computers running them, we cannot check the proof itself entirely by hand.

The reaction was not uniformly hostile. When Haken’s son presented his father’s work in a seminar at Berkeley, reports suggest the audience was divided pretty well by age. Those over forty were not prepared to accept a proof by computer, while those under forty felt that a computer proof was preferable to a 700-page hand proof, which they felt was less likely to be correct. So your attitude to computer proof may depend on your age!

The Four Colour Problem is not the only long-outstanding mathematical conjecture to have yielded to the computer. An even older problem is the Kepler Conjecture, dating back to the beginning of the seventeenth century. The great scientist Johannes Kepler had been discussing how to stack spherical objects in correspondence with the English mathematician Thomas Harriot: their interest was in the packing of cannonballs on board ship. Kepler’s conjecture is that the most efficient way to stack spheres is the way you will find oranges set out in your local greengrocer: the bottom layer is set out in a square lattice and the next layer is inserted into the gaps in the natural way. This layout, which I will call the greengrocer’s arrangement, seems to be the most efficient packing, in terms of maximising the density of oranges and minimising the wasted space between them, but is it the best?

(Another contender is hexagonal packing, but if you have better three-dimensional visualisation powers than I do, you can see that this is simply the same arrangement viewed from a different angle.)

Newton worked on the problem, and Gauss showed in 1831 that the greengrocer’s arrangement is best if one requires that the packing form a regular lattice. But might an irregular packing be denser? In 1900, David Hilbert included this problem in his list of twenty-three unsolved mathematical problems that set the agenda for twentieth-century mathematicians.

The next breakthrough came in 1953 when László Tóth showed that the problem could be reduced to a finite (but enormous) set of calculations. At the beginning of the 1990s Thomas Hales showed that the problem could be solved by minimising a certain function of 150 variables. He then addressed this using specialist mathematical software for minimising such functions – the method is called linear programming. By examining 5000 different configurations of spheres, which meant solving 100,000 linear programming problems, he claims that, with extensive use of this software, he has proved the conjecture that the greengrocer’s method is best.

Hales’s initial proof ran to 250 pages along with — and this is the difficult bit — 3 gigabytes of computer data. After several years work, referees said they were 99% satisfied of its correctness. Parts of the proof were published in a leading journal, but in the end the journal (understandably) couldn’t find referees prepared to sacrifice the time necessary to check the work fully. (We’ll come back to this point in a moment.)

Where Hales’s proof of the Kepler conjecture differs from the computer proof of the Four Colour Theorem is in the nature of the computer software used. While Appel and Haken used bespoke software, which could to some extent be checked, Hales relied on standard linear programming software which is of another order of complexity. While most mathematicians believe Hales’s proof is correct, it is a long way from a traditional mathematical proof that you or I could check for ourselves.

While these two examples — the Four Colour Theorem and the Kepler Conjecture — are cases where computers have assisted mathematicians in finding and verifying proofs, a fascinating area of contemporary computer science is the use of computers to construct complete proofs, and to find new results.

There have been some remarkable triumphs, although no computer has yet found a new theorem sensational enough to hit the headlines in the popular press. But results have been found, and there are websites where you can buy the naming rights to a new computer-discovered mathematical theorem.

One of the most important results of twentieth century mathematics is the Feit-Thompson Theorem. (The terms are technical but the nature of the achievement should be clear.) In 1911 the British mathematician William Burnside asked whether every group of odd order is soluble. This simple-sounding statement was finally proved...
by Walter Feit and John Thompson in 1962. Their paper was 255 pages long, which was unprecedented in the subject. And late in 2012 a team led by Georges Gonthier has formalised this proof in an interactive theorem-proving system called Coq: we now have a computer proof of the Feit-Thompson Theorem. Just to give a flavour for those who remember a little group theory, here is the computer representation of the structure of a finite group:

```
Structure finGroupType Type := FinGroupType { 
  element := finType; 
  1 : element; 
  -1 := element -> element; 
  * := element -> element -> element; 
  unitP : \forall x, 1 * x = x; 
  invP : \forall x, x^-1 * x = 1; 
  mulP : \forall x y z, (x * y) * z = x * (y * z);
}.
```

And here is the statement of the result:

```
Theorem Feit_Thompson (gT : finGroupType) (G : {group gT}) : odd #|G| -> solvable G.
```

Thomas Hales has written, “To me as a mathematician, nothing else that has been done by the formal proof community compares in splendor to the formalization of this theorem.”

Computers have contributed a great deal more to mathematics. In 1989 2000 hours of the time of a Cray supercomputer showed that there is no finite projective plane of order 10: the case n=12 however remains out of reach. Computers have also helped prove results such as the Catalan Conjecture, which states that the only non-trivial integer solution to the equation $x^m - y^n = 1$ is the simple $3^2 - 2^3 = 1$. Mihailescu’s proof in 2002 used one minute of computer time, and a subsequent proof has been found which doesn’t use computers at all. Computers have found counter-examples to conjectures: Euler’s suggestion that, in integers, an $n^{th}$ power cannot be the sum of $(n-1)$ $n^{th}$ powers was refuted by the computational discovery that $27^5 + 84^5 + 110^5 + 133^5 = 144^5$ and more recently a counter-example involving three fourth powers has been found.

Computers help mathematicians in many other ways. One obvious one is visualisation: computer images and animations have been enormously helpful in the mathematical development of chaos theory and non-linear dynamical systems, and many other fields of pure mathematics. For example, Gwyneth Stallard works with Julia sets in complex analysis and Caroline Series has studied the Maskit embedding in group theory.

Mathematicians have also used computers to test conjectures, and to examine examples which suggest ideas for theorems which can be investigated, and sometimes proved, by hand. The Birch and Swinnerton-Dyer Conjecture, one of the major outstanding mathematical problems and one for which you stand to win a million dollars from the Clay Institute if you prove it, was inspired by observation of computer calculations, and Sato was similarly inspired in proposing the Sato-Tate conjecture about elliptic curves.

But it’s not just through calculation that computers help mathematicians. A couple of years ago one of our leading mathematicians, the Fields Medallist Sir Timothy Gowers, told the British Mathematical Colloquium that one of the most useful tools for a working mathematician today is Wikipedia. While many academics are critical of, or even hostile to, Wikipedia, its mathematics content seems to be genuinely very reliable, accurate and useful. If you want to get into a new area of mathematics, Wikipedia is certainly the place to start, and not only because of its convenience. Online journals, and the arXiv where mathematicians post preprints of their papers, also play a huge role. Such ready access to these information sources brings considerable benefits to the profession.

In general the communications revolution has had a profound effect on the practice of mathematics. While mathematicians have always worked together, the pace of electronic communication has made possible new forms of collaboration. One example is Gowers’s “polymaths”. In January 2009 Gowers posted a major unsolved mathematical problem on his blog and invited collaboration from anyone who wished. Over 40 people joined in and the problem was solved in seven weeks: the pace was remarkable. Gowers suggested that whereas in the past fear of being anticipated led mathematicians to work privately, the public forum of the polymaths blog encourages the immediate sharing of ideas (with priority established by the blog posting) and makes large-scale collaborative work much more feasible. If he is right (and research funding mechanisms which don’t value massively collaborative work may push in the opposite direction), computer communications are profoundly changing the way mathematics is done.

So where is proof and mathematics? I think that in one respect the nature of proof has changed. In its time the
255-page proof of the Feit-Thompson Theorem was a monster, but it is now by no means unique. Many very important mathematical results have proofs which are accessible to very few, and to these only with great effort. (There are true mathematical statements whose shortest proof is arbitrarily long. One example, given by Gödel, is the statement “This statement has no proof in Peano arithmetic that contains fewer than $10^{1000}$ symbols.”) The idea that a mathematical proof is something which anyone can check for themselves no longer matches the reality of some present-day mathematics.

What happens when someone proposes a new proof? Well, generally the proof is peer-reviewed. But in 2004 the maverick mathematician Louis de Branges announced a proof of the Riemann Hypothesis, perhaps the greatest problem in mathematics, still unsolved after a century and a half. His proposed proof was 124 pages long, and I believe it is not entirely clear. The approach taken was not thought by the mathematical community to be likely to lead to a proof of the Riemann Hypothesis. De Branges’s “proof” does not appear to have been checked carefully by any of the mathematicians who are competent to evaluate it. Why should they spend time examining a proof they expected to be faulty when they could spend the time doing their own work on which their reputations (and funding) depend?

Why should de Branges be taken seriously? Well, he has form. In 1984 he announced a proof of the Bieberbach Conjecture in complex analysis, which had been unproved for almost 70 years. His proof seemed sketchy and incomplete, and was not initially accepted by his peers: but a group of mathematicians in Leningrad spent several months working on it and established that it was valid. Yet even with this track record, de Branges’s “proof” of the Riemann Hypothesis remains in limbo, lacking referees, not accepted but not refuted.

So it is hard to evaluate some of today’s proofs. The story of the Four Colour Theorem also shows us that errors in proofs can be undetected for some time - it was more than ten years before the problem with Kempe’s “proof” was spotted. Other proofs have contained errors, some fixable, and some not. There is even a Wikipedia page which lists important proofs which turned out to be incomplete. When I last looked, it gave 37 examples, of which 15 were correct results which have now been rigorously proved (we think), 10 were results which were incorrect as stated but where a modified version has been proved, seven proofs were wrong and unfixable, and the status of five is unclear. The mathematicians involved included such great names as Cauchy, Riemann, Lebesgue and Gödel! So there is plenty of evidence that human proofs are fallible. And with Gödel’s Theorems having shown us that in any useful logical system there are true statements which we cannot prove, and indeed that (roughly speaking) we cannot prove that mathematics is consistent, it is perhaps surprising that we still do maths in much the same way. The mathematician John von Neumann is said to have come out of a seminar by Gödel in 1930 saying “It’s all over”, implying that Gödel’s results were fatal to pure mathematics, yet we still prove things.

So where are we? I used to think it was ironic that we now consider as deluded these mathematicians of the 1880s who believed in the Four Colour Theorem on the basis of a simple proof that anyone could verify for oneself, subtly wrong though it turned out to be, whereas we are now confident in our superior knowledge of the veracity of the theorem on the basis of computer calculation that none of us could possibly check for oneself. But we are fallible, so perhaps computer proofs are more reliable?

We have to be careful! Here is a “Theorem” which some computer proof assistants can prove:

$$\exists n. n < 0 \land 0 < n$$

This seems to say that there exists an integer $n$ which has the property that $n$ is strictly less than zero, and also $n$ is strictly greater than zero. This statement is false. How do the proof systems prove it?

Well, what they are actually proving is the true statement that $\exists n. t < n$ which says that if you give me a number $t$, there exists a smaller number $n$. But instead of using the sensible name “$t$” for the free variable, they allow you to call it “$n < 0 \land 0'$”, a meaningless string which in this context can be confusing! So computer proofs don’t remove the possibility of ambiguity. (OK, that’s a rather frivolous example.)

But there is a bigger problem. In my previous lecture I discussed why computers make errors, due to mistakes by their human programmers and designers. But there is another source of computer errors, called “soft errors”. These are errors caused by, for example, cosmic rays, which can cause an alpha particle to change a value stored by a computer. Estimates suggest that a computer at sea level running for 77 hours (the time taken for a recent calculation in group theory) would expect to experience about 40 soft errors during that time. At higher altitudes errors would be significantly more frequent. This raises the question of how sure we can be of a computer proof when the data may have been corrupted mid-proof.

So experience has taught us that human mathematicians are fallible, and even correctly designed and programmed computers are liable to soft errors. Where does this leave mathematical proof? Thomas Hales, in his wonderful recent survey article on which this lecture has drawn extensively, says he “admits physical limits to the reliability of any verification process, whether by hand or machine. These limits taint even the simplest theorems, such as our ability to verify that $1 + 1 = 2$ is a consequence of a set of axioms. One rogue alpha particle brings all my schemes of perfection to nought.” The fallibility of the human mind and the physics of our universe both affect the viability of absolute mathematical proof.
What does this mean for the practising mathematician? In a popular lecture last year Sir Timothy Gowers predicted that in 25 years’ time computers will be useful assistants to pure mathematicians, and that in 50 years they will be doing mathematics better than humans. Should that happen, would pure mathematics still be of any interest to us?

This survey has looked at some anecdotes in the recent history of proof, both by human and by machine. (While I was writing this talk I was very much aware that female mathematicians didn’t feature in my historical examples: perhaps, since I have looked mainly at incomplete and faulty proofs, that just shows that women don’t make mistakes!) For 2300 years, ever since Euclid, proof has been central to mathematics, even if proofs have gone from simple demonstrations checkable by anybody to long technical expositions understandable only by a tiny number of specialists. With computers now proving theorems, mathematicians’ relationship with proof may be about to change again. Is mathematics still going to be about Dee’s “truthes certaine, necessary, and invincible: vnuersally and necessarily concluded”?

© Tony Mann 2013