Thought-Experiments: Proof in a Computer Environment

John Costello

Formalism and proof in mathematics education

For most of the twentieth century, the philosophy of mathematics has been dominated by a formalist view of the foundations of mathematics. According to this view, mathematical objects – sets, numbers, geometrical shapes and so on – exist only in a formal sense: they *are* the strings of symbols which denote and define them. Of course, these formal things can be used to model the real world; and such mathematical models give us a lot of power, both to understand the world better and to deal with it. But mathematics itself has no being beyond its formal representation: there is no Platonist universe in which abstractions exist.

Oddly enough, mathematicians *behave* as if abstractions have some external reality. They explore structures, numbers and geometrical configurations, and appear to make new discoveries through this exploration. On the face of it, there does not seem to be a great deal of difference between, say, the discovery that Uranus and Neptune have lots of satellites and the discovery that a particular set of large numbers are all prime. Astronomers, however, will reassure us that the moons really are out there somewhere. On the other hand, mathematicians when pressed are more likely to retreat into formalism: these numbers are no more than symbols – and their properties and relationships are all given to them through our axioms and definitions. Theorems are just logical tautologies, obtained from axioms and definitions by specified rules of inference.

It has to be like this. After all, if we start crediting abstractions with existence, we are on the way to putting them in some mystical environment outside our physical universe – and we can hardly have that, can we? Something of this dilemma is captured by Davis and Hersh [1], who write that 'the typical working mathematician is a Platonist on weekdays and a formalist on Sundays'.

The typical mathematics teacher, however, is in an almost directly opposite position. Frequently, classroom activity suggests that mathematics is being treated as a purely formal activity. A lot of school mathematics appears to involve the manipulation of strings of symbols. The rules of this manipulation can be learned and applied, without meaning being attached to the results.

Yet, despite appearances, formalism is educational heresy. Teachers believe in (and are committed to) things called 'concepts', which lie behind the formal language and symbolism. Take, for example, the topic of area. Lessons may involve calculating lots of areas, and learning methods and formulae relating to these calculations. But most teachers would argue that it is more important for pupils to understand what area *is*; and this is the philosophical giveaway. Area is a concept: it has an existence beyond the calculations and the manipulation of symbols. It is here that teachers part company so radically with the Davis and Hersh description of mathematics: teachers may behave like formalists a lot of the time but their philosophical standpoint is closer to Platonism.

When it comes to proof in mathematics education, however, the emphasis is all on formalism. The only genuine proof is a formal proof. This is all about writing symbols in a precise and standard order, about imposing a logical, consistent structure on the whole of mathematics. There are of course teachers who will argue that proof is a personal matter or that it is very dependent on culture and context; but it is hard to find good examples of this philosophy in practice.

The formalist agenda of twentieth century mathematics has been enormously powerful in promoting the systematisation of mathematics into a standard deductive structure. In his own introduction to *Proofs and Refutations*, Lakatos [2] expressed it like this:

It frequently happens in the history of thought that when a powerful new method emerges the study of those problems which can be dealt with by the new method advances rapidly and attracts the limelight, while the rest *tends to be ignored or even forgotten, its study despised.*

If this statement were written out of context, by itself on the page, we would be unlikely to guess correctly what it is talking about. It feels a lot more like a statement about computers than about formalist philosophy. So here is an unexpected parallel. Computers provide a powerful new way of dealing with mathematics. For most of this century, a formalist programme has had comparable (although very different) power. The place of proof in the formal structure has been relatively clear. So what difference do computers make?

The logical formalist approach is entirely synthetic. It disconnects mathematics from its history and its psychology. It presents, orders, develops and justifies mathematical knowledge in a systematic way, which is quite different from the way in which that knowledge was created historically and the way in which it is learned. This approach imposes a detailed structure on mathematics. It makes it almost impossible for the learner to construct proofs rather than simply learn them, because the place of any result in the mathematical hierarchy is so tightly constrained. Yet we know very well that students and even young children can appreciate proof and argue deductively. Such proof has little to do with formal systematisation: it is about how you know something is always true, and how you convince yourself and other people.

Lakatos offers a model of proof as a 'thought-experiment'. This is an ancient pattern of mathematical proof, known in pre-Euclidean Greek mathematics as *deiknymi*. The detailed illustration in *Proofs and Refutations* is the relationship V+F-E = 2, relating the vertices, edges and faces of a polyhedron. How might we develop this theorem? Well, first we look at a few particular polyhedra, count their vertices, faces and edges and formulate a rule connecting these. Then we think up a thought-experiment to justify the rule in general.

This is the thought-experiment. We take hold of our polyhedron and make a hole in one of its faces. Now, we pull and stretch out the hole until the polyhedron is flattened out into a network. Next we triangulate this network, and then we dismantle it, one arc at a time, until we get down to a single triangle. All the time, we have to check that these processes do not change the value of V+F-E.

There are two things to say about this proof. One is that it is accessible. It needs explanation and thinking about, but it is intuitive and self-contained. It does not depend on lots of axioms, lemmas, theorems and rules of inference. The second important comment is that this result is not obvious to start with. It needs a few particular examples to make it plausible, and then the need for a general proof is easy to appreciate. This combination of non-obviousness and accessibility makes the result *wonderful*.

The word is chosen carefully. At the 1994 ATM conference, Johnston Anderston conducted a discussion on the seven wonders of the (mathematical) world. The F+V-E = 2 formula was not voted into the seven, but it was mentioned. And it was clear that the suggested criteria for wonderfulness were being used. For example, the unique factorisation theorem for integers into primes was not a candidate: it does not seem to need proof. It is obvious that you can break down any integer uniquely in this way, and the proofs usually offered are less convincing than intuition. On the other hand, the infinitude of the prime numbers *is* wonderful. It is not obvious – indeed it is in some ways counter-intuitive – but the proof is simple and accessible. Well, fairly accessible anyway. The only possible stumbling block is the rule of inference which allows proof by contradiction: the proof is usually presented in this way. We'll return to this question later.

Justification and proof in computer micro-worlds

In secondary schools, the use of Logo to produce polygons is a familiar task. Commonly the turtle moves forward all round the polygon, so that the focus of attention is the turning or exterior angle at each vertex. It is a very simple matter to see that these must add up to one complete turn. As an approach to the interior angles this is somewhat indirect. To show, for example, that the angles of a triangle add up to a half-turn by this method is a bit contrived, although it is probably more accessible than a proof based on constructions and properties of parallel lines, which really belongs to the formal Euclidean system.

Of course there is no real reason why the turns should not be the interior angles. But there is something about the image of the turtle which makes this seem unnatural. To get round the triangle turning through interior angles, the poor turtle has to crawl up to the first vertex, then swing its backside through the interior angle before backing along the next side. On the other hand, this startling thought-experiment does make it very clear that the total turn through the three interior angles is half a complete turn.

Similar perspectives can make other geometrical relationships, such as the properties of alternate and corresponding angles, very obvious. One of the challenges of using computers in mathematics education is to create micro-worlds which make this obviousness accessible.

It is unsurprising that a computer graphics facility should generate a particular kind of geometrical proof. After all, its purpose is to explore the properties of shape, and the features of the specific micro-world encourage certain forms of thought-experiment. It is a little more difficult to apply these ideas to properties of numbers. Suppose, for example, we want to make the infinitude of the prime numbers obvious and accessible. As presented in most text-books, the standard proof depends on *reductio ad absurdum*. A useful exercise is to produce a constructive proof. In computer terms, we want to write a procedure (maybe in Logo or in some other programming language) which will continue to generate new primes.

Of course it is not all that difficult to write a program which checks numbers for divisions and prints out a list of all the primes in order as far as is required. But this begs the question. We know that primes will keep churning out only because we know that there are infinitely many of them anyway. What we want is a recursive procedure which will always and obviously produce another prime within a finite (specifiable) number of steps.

There are plenty of ways to tackle this. One way is to capture the spirit of the classical proof by accumulating a list of primes p1, ... pr and producing the next one by calculating p1 p2 ... pr + 1 and obtaining its *smallest prime factor* by division. If we start this sequence with 2, it becomes:

2, 3, 7, 43, 13, 53, ...
(because 13 = 1807 ÷ 139 and 53 = 23479 ÷ 443)

Starting with 3 (or 7) makes no difference:

3, 2, 7, 43, 13, 53, ...   7, 2, 3, 43, 13, 53, ...

But starting with 5 gives:
5, 2, 11, 3, 331, 19, . . .

These sequences do not contain *all* the primes (at least I don't think they do), but they are infinite sequences of primes, in which each new term is generated in a clearly finite number of steps.

As a computer algorithm for generating primes, this procedure has some disadvantages. Never-the-less, it is worth consideration and investigation. We know that there are infinitely many primes because of a subtle piece of dialectic: for those who appreciate such logic, this may be exciting, but many simply learn about it and have no further use for it. The activity suggested here is a way of establishing ownership of this knowledge, and of developing individual alternative formulations of the proof.

It may be helpful to try to find some metaphor or imagery, to understand the function of the computer and the micro-world it provides, in doing mathematics and working on mathematical proof.

In some sense, a micro-world is a neo-Platonist universe. It is a place where geometrical shapes, numbers and other mathematical entities exist in their own right, and can be explored. This, however, is a little pretentious in tone: perhaps the analogy of a chess-board is better.

It is sometimes said that formal mathematics is just a complicated game, like an elaborate form of chess. The objectives of this game are various kinds of *completion*: for example, problems are *solved* and theorems are *proved*. Becoming good at mathematics involves learning to achieve these objectives and recognising when they are completed correctly. A micro-world is a visually accessible and easily manipulated arena in which this game can be played.

The comparison with chess goes something like this. Imagine trying to explain chess with no board and no pieces. A purely formal notation is used to write down the moves, the rules are described in words, and somehow you have to try to understand when and how the game is complete. Until the advent of computers, this is how we have been doing mathematics. Now, computers provide us with the board. This extreme view will not appeal to everyone. But it is breathtaking to speculate that future generations may look back in amazement at mathematics in the pre-computer age and at how this most elaborate game was played without the essential equipment.

Limitations of micro-worlds

Sometimes the boundaries of a micro-world are plain to see. On other occasions it may take a long time to find these limitations. In some cases we find not so much limitations as anomalies: the micro-world turns out to have its own structure and properties which are not quite those of the system that we expected, or perhaps intended it to represent. There is a curious illustration of this in the appearance of ambiguous and impossible objects in *3D-Logo* [3]. These considerations raise the question of whether it can ever be possible to create a computer micro-world which provides a self-contained, consistent and complete system of representing space or number.

Any software can challenge us to find some application which the authors did not envisage; and we are especially delighted then if something weird happens. Sometimes it may be not so much that the micro-world is unsound; rather it may create a whole new system of its own. This is probably most obvious in graphical work, but there are numerical illustrations too, especially when the outcome of a procedure is particularly sensitive to rounding errors and to the degree of precision of the arithmetic.

Of course, in any particular situation, clever software designers will refine the facility so that we can model and investigate the *exact* behaviour of the structure. Then we shall have to find something else to thwart the system – and we will always be able to do this.

Computer-generated proofs

The most disquieting aspect of the use of computers in mathematics is not their limitations and inadequacies: indeed it would be somewhat consoling to believe that no micro-world could ever provide a complete, self-contained representation of number or geometry. What causes most unease is the notion that some mathematical proofs can depend entirely on the use of computers. The most quoted illustration of this is the four-colour theorem, but there are many truths which we know only because of computer procedures. For example,

$2^{21701} - 1$ is prime.

Probably you believe this. You can be fairly sure, too, that no human being has carried out all the calculations required to confirm it. If I quote for you the date and place that this result was checked by computer, it will not upset you, but you will not be thrilled by it either. And this is the point. You never expected this result to be *wonderful*. I could make it wonderful, if I could in a two-or-three-line thought-experiment, make it obvious. Then, you might get excited, and start trying to apply my thought-experiment to some more big numbers. Unfortunately I cannot offer you the opportunity.

Now let's go back to the four-colour theorem. This is a real let-down. We want a clever, accessible thought-experiment, like the proof of Euler's formula for polyhedra. Instead of this, we have an inaccessible computer-based proof.

Computers have enormous influence on the accessibility of mathematics. They can give us a universe within which to explore mathematics and make the truth of mathematical statements obvious and accessible to each of us in an individual way. Yet they also allow mathematicians to create proofs which are not (and never can be) accessible to anyone. Given the pervasive contemporary usage of computers, it is clear that more and more new aspects of mathematics – new knowledge, if you like, or new truths – are going to be computer-generated.

It is worth reflecting that the powerful new methods provided by the formalist approach to the foundations of mathematics in the early twentieth century did not generate accessible proofs. In the work of Whitehead and Russell [4], a proof might consist of pages full of strings of symbols painstakingly transformed by careful rules of inference. We might in some sense be reassured because someone has set up the basic structure of mathematics in this way. But its real effect on our understanding is hardly more significant than that of modern computer proofs.

For those who continue to find excitement and enthusiasm in teaching and learning mathematics, proof is an important part of the package. We need to ask ourselves why. We might mention aesthetic aspects of proof, insight and elegance. We might talk about constructing proofs, convincing ourselves and other people, and making mathematical knowledge our own. These matters have very little to do with axioms, rules of inference and the systematisation of mathematics. On the contrary, our concern is almost entirely with thought-experiments.

The delight which we find in such proofs has survived the stultifying hand of formalism, and it will equally survive the pressures of the computer age. Some mathematicians will produce computer-generated proofs of new theorems. Others, however, may use computer micro-worlds to provide new, accessible proofs of old theorems. In this way, the theorems will become not just true but obvious and wonderful.

John Costello works at Loughborough University.

References

1. Davis, P J and Hersh, R (1983), *The Mathematical Experience*, Penguin.
2. Lakatos, I (1976), *Proofs and Refutations*, Cambridge University Press.
3. Costello, J (1994), Ambiguous cubes, *Micromath*, 10(1).
4. Whitehead, A N and Russell B (1910-), *Principia Mathematica*, Cambridge University Press.