SEMI-AUTOMATED THEOREM PROVING

—

THE IMPACT OF COMPUTERS ON RESEARCH IN PURE MATHEMATICS

Marston Conder

Department of Mathematics, The University of Auckland

Private Bag 92019, Auckland, NEW ZEALAND

e-mail: conder@mat.auckland.ac.nz

1 Introduction

There is no doubt that the use of computers in recent years has revolutionised many branches of science, not the least of these being mathematics. Even in pure mathematics, where often quite subtle and sophisticated arguments are required for the solution of problems, computers have become an invaluable, almost indispensible tool.

In this paper I will describe in more detail some aspects of the impact of computing on research in pure mathematics, and in particular on the use of specialist software to solve mathematical problems.

I will briefly discuss computer-based proofs with reference to two famous examples: the 4-colour theorem, and the non-existence of a projective plane of order 10, and will also mention a few of the major developments within mathematics that have resulted from the influence of computing. Finally I will outline some of the ways in which I have used computer software in my own research, with the aim of illustrating the potential of experimental approaches to questions in pure mathematics.

To begin with, however, it is appropriate to make some general comments. First, it may be said that computers were originally developed to perform calculations which were essentially pure mathematics, and hence it is natural that they continue to be used in this area. On the other hand, their use will always be limited, for by Turing's 1936 answer to Hilbert's 3rd problem, there can be no *universal machine* to decide the truth or falsity of every mathematical statement.

Since the design of computers for cracking secret cyphers in World War II, major areas and directions of pure mathematics have altered considerably. The renaissance of number theory (through cryptography) is a notable example, and others include matrix algebra (resulting from extensive research on the solution of linear and differential equations) and combinatorics. More generally, we have witnessed a gradual *discretization* of pure mathematics, although not necessarily at the expense of continuous mathematics.

Computer-based proofs have become common, if not always popular, and much effort is being poured into the areas of constructive mathematics, algorithms, special-purpose mathematical software, and experimental pure mathematics. Some of these will be dealt with in the following two sections.

2 Computer proofs

In recent years a number of long-standing questions and conjectures in pure mathematics have been settled: the Four Colour Theorem, Mordell's conjecture, the Bieberbach conjecture, and of course Fermat's Last Theorem. Of these perhaps the proof of the Four Colour Theorem has been the most controversial, in that the use of a computer was necessary to complete it. Here are some observations about this and another example of interest:

Example 2.1: The Four Colour Theorem

The Four Colour Theorem (or 4CT for short) states that *only 4 colours are required to colour the regions of any plane map in such a way that every two neighbouring regions have different colours.* This was conjectured by Guthrie in 1852, and had a long history of fallacious "proofs" (and attempted proofs), until it was settled with the help of a computer in 1976.

Appel and Haken's proof [AH] came in two parts: Part I being a classification of *unavoidable configurations,* and Part II verifying the reducibility of each configuration (to show there is no minimal counterexample). Part I involved enumeration by hand of some 1400 cases, while Part II used a computer to verify reducibility in each case.

Ironically Part II caused the most controversy, with many eminent and highly-respected mathematicians raising the possibility of computer errors, yet Part I was much more prone to human error — and some say Part I has never been independently verified!

Nevertheless the 4CT is now believed to be true, and in 1994 a simpler proof was constructed by Robertson, Sanders, Seymour and Thomas [RS], replacing Part I of Appel and Haken's proof by a machine-readable and verifiable list of 633 cases.

Example 2.2: There is no projective plane of order 10

A finite projective plane of order n is an incidence structure made up of n^2+n+1 points and n^2+n+1 lines, such that any two points lie together on exactly one line and any two lines intersect in exactly one point. Such a plane is known to exist whenever n is a prime-power, however there is no *known* plane of non prime-power order n.

It was proved by Tarry in 1900 that there is no projective plane of order 6, but it then took until 1989 to show there is no projective plane of order 10. This was achieved by Lam, Thiel and Swiercz [LT], using a computer search for 19-point configurations (corresponding to codewords of length 19 in the associated binary code).

Their search required over 2000 hours of computing time, with the obvious implication of hardware errors. In fact they admit the detection and correction of such errors, but included checks in their programming so that even with one error per 1000 hours, the probability of their proof being incorrect would be at most 1 in $500,000$.

Example 2.1 indicates a change in the interpretation of "proof", where we may accept a result as being *very probably* true. In a similar vein, a general desire to understand how and why some theorems are true — rather than proving by contradiction that they cannot be false — has stimulated

the growing field of *constructive mathematics.*

Along with this is a growth industry in automated reasoning (artificial intelligence), but also there has been a fundamental change of emphasis in methodology. Probabilistic and experimental techniques (using random number generation) are now common, and have even appeared in some aspects of pure mathematics.

Also with the advent of computers the need has been recognised for polynomial-time algorithms for solving problems. For a simple instance of this, note that when solving large systems of linear equations, the method of Gaussian elimination is far more efficient than Cramer's rule!

In turn new areas of mathematical research have been spawned, so much so that now one of the burning questions in mathematics concerns the relationship between problems which are polynomial-time solvable (P), and a class of those which are polynomial-time verifiable but not known to be polynomial-time solvable (NP): is $P = NP$?

3 Experimental mathematics & software

It is clear that mathematics has benefitted a great deal from the use and influence of computers. Apart from practical considerations and the wealth of new methods available, there is now a much greater understanding of many avenues of research.

Of course, computers are unlikely to ever match the ingenuity and creativity of the human mind, and quite rightly, "computer proofs" may always be viewed with some skepticism, but that should not detract from their potential to contribute in many significant ways. In particular, there are many situations in which a positive computational approach can yield new results or throw light on old problems.

Computers can be used for simulation (of systems and processes), combinatorial searches, construction and analysis of simple examples, formulation and testing of conjectures, and classification of small cases, for example. In such ways they can often provide answers that can subsequently be checked by hand, or provide a picture that points the way to a theoretical proof, as

will be illustrated in the next Section.

This form of experimental approach is becoming more common (and successful) in a large number of areas, especially number theory, discrete algebra, combinatorics, numerical computation, finite geometry, low-dimensional topology, and even statistical mechanics.

Many software packages are available, including special purpose packages Magma (for discrete algebra and number theory), GAP (groups, algorithms, programming), KANT and Pari (number theory), as well as more general purpose mathematical packages such as Maple, Mathematica, and MatLab. Such packages are now widely used in teaching and research, with considerable success, in many parts of the world.

4 Some recent examples & successes

In this section I will describe three examples of ways in which I have used computer methods in my own research, to illustrate some of the potential of the approaches suggested in Section 3.

Example 4.1: hexagon-free subgraphs of hypercubes

For every positive integer n, the hypercube Q_n is an incidence structure generalising the cube to n dimensions. Its vertices are all possible n-tuples of 0's and 1's (of which there are 2^n), and any two such n-tuples are joined by an edge whenever they differ in exactly one co-ordinate.

Some years ago Paul Erdös raised the following question (which is relevant to the study of fault tolerance properties of parallel-processing architectures): Can the edges of the n-cube Q_n always be coloured using t different colours in such a way that there is no hexagon whose edges all have the same colour? By a "hexagon" is meant a circuit of length 6, such as the one with vertices $(0,0,0)$, $(0,0,1)$, $(0,1,1)$, $(0,1,0)$, $(1,1,0)$, $(1,0,0)$, and the question entails finding some t (independent of n) for which a t-colouring exists.

When I first learnt about this question, I experimented with a few possibilities for suitable colourings, with the help of the GAP package in testing them for small values of n. Eventually I stumbled on the following idea:

Consider a typical edge of Q_n, from the vertex $\mathbf{x} = (x_1, \ldots, x_i, \ldots, x_n)$ to the vertex $\mathbf{y} = (x_1, \ldots, \bar{x}_i, \ldots, x_n)$, where $\bar{x}_i = 1 - x_i$. If $\mathbf{x}$ has L 1's to the left of x_i and R 1's to the right of x_i, then let us colour the edge $\mathbf{x} - \mathbf{y}$

$$\begin{cases} \text{blue} & \text{if} \quad L - R \equiv 0 \bmod 3 \\ \text{green} & \text{if} \quad L - R \equiv 1 \bmod 3 \\ \text{red} & \text{if} \quad L - R \equiv 2 \bmod 3 \, . \end{cases}$$

With this colouring, computation in small cases revealed no monochromatic hexagons, and then it was a relatively simple matter to prove (by hand) that for all n there are no monochromatic quadrangles or hexagons; see [C3].

Example 4.2: highly symmetric networks

A combinatorial graph (or network) Γ is said to be *symmetric* if any two ordered edges are equivalent under some symmetry of Γ, and more generally, *s-arc-transitive* if any two ordered paths of length s are equivalent under some symmetry of Γ. For example, the underlying graph of the 3-dimensional cube is 2-arc-transitive (but not 3-arc-transitive). More highly symmetric examples include the 3-arc-transitive Petersen graph (on 10 vertices) and Tutte's 5-arc-transitive 8-cage (on 30 vertices).

Several years ago Tutte proved that every symmetric finite *cubic* (trivalent) graph is at best 5-arc-transitive. Furthermore, Tutte's analysis shows that the symmetry group of any 5-arc-transitive finite cubic graph has to be a homomorphic image of a particular abstract group G_5, which may be presented in terms of generators and relations as follows:

$$G_5 = \langle\, h, a, p, q, r, s \mid h^3 = a^2 = p^2 = [p, q] = [p, s] = pqrsrs = a^{-1}paq = a^{-1}ras = h^{-1}php = h^{-1}qhr = h^{-1}rhpqr = hshs = 1 \,\rangle.$$

Conversely, any non-degenerate finite image of G_5 is the symmetry group of some 5-arc-transitive cubic graph.

Now computer methods exist for finding small images of finitely-presented groups such as G_5 (through their low index subgroups). Using such methods, Peter Lorimer and I were able to find several interesting examples of symmetric cubic graphs, providing answers to some long-standing questions; see [CL]. Subsequent identification of some of the common features of these examples was the key to the construction of an infinite family of 5-arc-transitive cubic graphs, dispelling any idea that such graphs are rare; see [C1].

Example 4.3: an unexpected isomorphism

Earlier attempts to find and analyse examples of symmetric graphs often involved the imposition of additional assumptions such as the presence of circuits whose vertices are permuted in cycles. In particular, associated with certain 4-arc-transitive graphs containing a circuit of length 12 was the group

$$4^+(a^{12}) = \langle\, h, a, p, q, r \mid h^3 = a^2 = p^2 = [p,q] = pqrqr = a^{-1}pap = \\ a^{-1}qar = h^{-1}phq = h^{-1}qhpq = hrhr = (ha)^{12} = 1 \,\rangle.$$

This group became the subject of attention for some time following several attempts to prove it is infinite.

Again computer methods revealed some aspects of its structure, and in particular I noticed a normal subgroup of index 336 with remarkable properties. Using this subgroup I was able to construct an 8×8 matrix representation of $4^+(a^{12})$, and further computation showed that modulo small primes $p \equiv 2, 3$ and 5, these 8×8 matrices generate a group of order $2p^3(p^3-1)(p+1)$, which happens to be twice the order of the 3×3 matrix group $SL(3,p)$.

In turn this observation led to the following theorem, which can be proved by hand (but which was discovered as a result of computer experimentation):

The group $4^+(a^{12})$ *is isomorphic to* $SL(3,\mathbb{Z}).C_2$*, the group of all* 3×3 *integer matrices of determinant* 1 *extended by its inverse-transpose automorphism.*

For the details, see [C2]. Incidentally, the reason underlying this unexpected isomorphism has been shown by Peter Neumann to have a connection with finite projective planes; but that is another story!

References

[AH] K. Appel and W. Haken, Every planar map is four colorable, Parts I & II, *Illinois J. Math.* **21** (1977), 429–567.

[C1] M. Conder, An infinite family of 5-arc-transitive cubic graphs, *Ars Combinatoria* **25A** (1988), 95–108.

[C2] M. Conder, A surprising isomorphism, *Journal of Algebra* **129** (1990), 494–501.

[C3] M. Conder, Hexagon free subgraphs of hypercubes, *J. Graph Theory* **17** (1993), 477–479.

[CL] M. Conder and P. Lorimer, Automorphism groups of symmetric graphs of valency 3, *J. Combinatorial Theory Ser. B* **47** (1989), 60–72.

[LT] C. Lam, L. Thiel and S. Swiercz, The non-existence of finite projective planes of order 10, *Canadian J. Math.* **41** (1989), 1117–1123.

[RS] N. Robertson, D. Saunders, P. Seymour and R. Thomas, The four-colour theorem, *preprint*.