Combinatorics entering the third millennium

Peter J. Cameron

Third draft, July 2001

Henry Whitehead reportedly said, "Combinatorics is the slums of topology".[1] This prejudice, the view that combinatorics is quite different from 'real mathematics', was not uncommon in the twentieth century, among popular expositors as well as professionals. In his biography of Srinivasa Ramanujan, Robert Kanigel [18] describes Percy MacMahon in these terms:

> [MacMahon's] expertise lay in combinatorics, a sort of glorified dice-throwing, and in it he had made contributions original enough to be named a Fellow of the Royal Society.

In the later part of the century, attitudes changed. When the 1998 film *Good Will Hunting* featured a famous mathematician at the Massachusetts Institute of Technology who had won a Fields Medal for combinatorics, many found this somewhat unbelievable.[2] However, life followed art in this case when, later in the same year, Fields Medals were awarded to Richard Borcherds and Tim Gowers for work much of which was in combinatorics.

In this chapter, I have attempted to tease apart some of the interrelated reasons for this change, and perhaps to throw some light on present trends and future directions. I have divided the causes into four groups: the influence of the computer; the growing sophistication of combinatorics; its strengthening links with the rest of mathematics; and wider changes in society. I have told the story mostly through examples. If the views and examples are somewhat personal, perhaps this is better than having no views at all.

[1] My attribution is confirmed by Graham Higman, a student of Whitehead.

[2] The "unsolvable math problem" is based on the actual experience of George B. Dantzig, who as a student solved two problems posed by Jerzy Neyman at Berkeley in 1940: see Brunvald [6].

1 The influence of the computer

Even before electronic computers had been built, theoretical issues led to important mathematics. Kurt Gödel [12] showed that there are true statements about the natural numbers which cannot be deduced from the axioms of a standard system such as Peano's. This result was highly significant for the foundations of mathematics, but Gödel's unprovable statement itself had no mathematical significance. The first example of a natural mathematical statement which is unprovable in Peano arithmetic was discovered by Paris and Harrington [24], and is a theorem in combinatorics (it is a slight strengthening of Ramsey's theorem). It is unprovable from the axioms because the corresponding 'Paris–Harrington function' grows faster than any provably computable function. Several further examples of this phenomenon have been discovered, mostly combinatorial in nature. (I note in passing that calculating precise values for Ramsey numbers, or even close estimates, appears to be one of the most fiendishly difficult open combinatorial problems.)

More recently, attention has turned from *computability* to *computational complexity*: given that something can be computed, what resources (time, memory, etc.) are required for the computation. A class of problems is said to be *polynomial-time computable*, or in P, if any instance can be solved in a number of steps bounded by a polynomial in the input size. A class is in NP if the same assertion holds if we are allowed to make a number of lucky guesses (or, what amounts to the same thing, if a proposed solution can be checked in a polynomial number of steps). The great unsolved problem of complexity theory asks:

$$\text{Is } \mathsf{P} = \mathsf{NP}?$$

On 24 May 2000, the Clay Mathematical Institute announced a list of seven unsolved problems, for each of which a prize of one million dollars was offered. The $\mathsf{P} = \mathsf{NP}$ problem was the first on the list [8].

This problem is particularly important for combinatorics since many intractable combinatorial problems (including the existence of a Hamiltonian cycle in a graph) are known to be in NP. In the unlikely event of an affirmative solution, 'fast' algorithms would exist for all these problems.

Now we turn to the practical use of computers.

Computer systems such as GAP [11] have been developed, which can treat algebraic or combinatorial objects, such as a group or a graph, in a way similar to the handling of complex numbers or matrices in more traditional systems. These give the mathematician a very powerful tool for exploring structures and testing (or even formulating) conjectures.

But what has caught the public eye is the use of computers to prove theorems. This was dramatically the case in 1976 when Kenneth Appel and Wolfgang Haken [1] announced that they had proved the Four-Colour Theorem by computer. Their announcement started a wide discussion over whether a computer proof is really a 'proof' at all: see, for example, Swart [31] and Tymoczko [35] for contemporary responses. An even more massive computation by Clement Lam and his co-workers [20], discussed by Lam in [19], showed the non-existence of a projective plane of order 10.

Computers have been used in other parts of mathematics. For example, in the Classification of Finite Simple Groups (discussed below), many of the sporadic simple groups were constructed with the help of computers. What distinguishes its use in combinatorics? Is it that, in a sense, the effort of the proof consists mainly in detailed case analysis, and so the computer does most of the work?

Finally, the advent of computers has given rise to many new areas of mathematics related to the processing and transmission of data. Since computers are digital, these areas are naturally related to combinatorics. They include coding theory (discussed below), cryptography, integer programming, optimisation, constraint satisfaction, and several others.

2 The internal state

The last two centuries of mathematics have been dominated by the trend towards axiomatisation. A structure which fails to satisfy the axioms is not to be considered. (As one of my colleagues put it to a student in a class, "For a ring to pass the exam, it has to get 100%".) Combinatorics has never fitted this pattern very well.

When Gian-Carlo Rota and various co-workers wrote an influential series of papers with the title 'On the foundations of combinatorial theory' in the 1960s and 1970s (see [28, 9], for example), one reviewer compared combinatorialists to nomads on the steppes who had not managed to construct the cities in which other mathematicians dwell, and expressed the hope that these papers would at least found a thriving settlement.

While Rota's papers have been very influential, this view has not prevailed. To see this, we turn to the more recent series on 'Graph minors' by Robertson and Seymour [27]. These are devoted to the proof of a single major theorem, that a minor-closed class of graphs is determined by finitely many excluded minors.

Along the way, a rich tapestry is woven, which is descriptive (giving a topological embedding of graphs) and algorithmic (showing that many graph problems lie in P) as well as deductive.

The work of Robertson and Seymour and its continuation is certainly one of the major themes in graph theory at present, and has contributed to a shorter proof of the Four-Colour Theorem. Perhaps it will lead to new insights on such famous problems as Hadwiger's Conjecture and the Strong Perfect Graph Conjecture in the future.

What is clear, though, is that combinatorics will continue to elude attempts at formal specification.

3 Relations with mathematics

In 1974, an Advanced Study Institute on Combinatorics was held at Nijenrode, the Netherlands, organised by Marshall Hall and Jack van Lint. This was one of the first presentations, aimed at young researchers, of combinatorics as a mature mathematical discipline. The subject was divided into five sections: theory of designs, finite geometry, coding theory, graph theory, and combinatorial group theory.

It is very striking to look at the four papers in coding theory [15]. This was the youngest of the sections, having begun with the work of Hamming and Golay in the late 1940s. Yet the methods being used involved the most sophisticated mathematics: invariant theory, harmonic analysis, Gauss sums, Diophantine equations.

This trend has continued. In the 1970s, the Russian school (notably Goppa, Manin, and Vladut) developed links between coding theory and algebraic geometry (specifically, divisors on algebraic curves). These links were definitely 'two-way', and both subjects benefited. More recently, codes over rings and quantum codes have revitalised the subject and made new connections with ring theory and group theory.

Another example is provided by the most exciting development in mathematics in the late 1980s, which grew from the work of Vaughan Jones, for which he received a Fields Medal in 1990. His research on traces of Von Neumann algebras came together with representations of the Artin braid group to yield a new invariant of knots, with ramifications in mathematical physics and elsewhere. (See the citation by Joan Birman [3] and her popular account [4] for a map of this territory.) Later, it was pointed out that the Jones polynomial is a specialisation of the Tutte polynomial, which had been defined for arbitrary graphs by Tutte and Whitney and generalised to matroids by Tutte. Tutte himself has given two accounts of his discovery: [33, 34]. The connections led to further work. There was the work of François Jaeger [17], who derived a spin model, and hence an evaluation of the Kauffman polynomial, from the strongly regular graph associated with the Higman–Sims simple group; and that of Dominic Welsh and his collaborators (described in his book [36]) on the computational complexity of the new knot invariants.

Examples such as this of unexpected connections, by their nature, cannot be predicted. However, combinatorics is likely to be involved in such discoveries: it seems that deep links in mathematics often reveal themselves in combinatorial patterns.

One of the best example concerns the ubiquity of the Coxeter–Dynkin diagrams A_n, D_n, E_6, E_7, E_8. Arnol'd (see [7]) proposed finding an explanation of their ubiquity as a modern equivalent of a Hilbert problem, to guide the development of mathematics. He noted their occurrence in areas such as Lie algebras (the simple Lie algebras over $\mathbb{C}$), Euclidean geometry (root systems), group theory (Coxeter groups), representation theory (algebras of finite representation type), and singularity theory (singularities with definite intersection form), as well as their connection with the regular polyhedra. To this list could be added mathematical physics (instantons) and combinatorics (graphs with least eigenvalue -2). Indeed, graph theory provides the most striking specification of the diagrams: they are just the connected graphs with all eigenvalues smaller than 2.

Other developments include the relationship of combinatorics to finite group theory. The Classification of Finite Simple Groups [13] is the greatest collaborative effort ever in mathematics, running to about 15000 journal pages. (Ironically, although the theorem was announced in 1980, the proof contained a gap which has only just been filled.) Combinatorial ideas (graphs, designs, codes, geometries) were involved in the proof: perhaps most notably, the classification of spherical buildings by Jacques Tits [32]. Also, the result has had a great impact in combinatorics, with consequences both for symmetric objects such as graphs and designs (see the survey by Praeger [26]), and (more surprisingly) elsewhere as in Luks' proof [22] that the graph isomorphism problem for graphs of bounded valency is in P.

This account would not be complete without a mention of the work of Richard Borcherds [5] on 'monstrous moonshine', connecting the Golay code, the Leech lattice, and the Monster simple group with generalised Kac–Moody algebras and vertex operators in mathematical physics and throwing up a number of product identities of the kind familiar from the classic work of Jacobi and others.

4 In science and in society

Like any human endeavour, combinatorics has been affected by the great changes in society last century. The first influence to be mentioned is a single individual, Paul Erdős, who is the subject of two recent best-selling biographies [16, 29].

Erdős' mathematical interests were wide, but combinatorics was central to them. He spent a large part of his life without a permanent abode, travelling the world and collaborating with hundreds of mathematicians. In the days before email, he was a vital communication link between mathematicians in the East and West; he also inspired a vast body of research (his 1500 papers dwarf the output of any other modern mathematician).

Jerry Grossman [14] has demonstrated the growth in multi-author mathematical papers this century, and how Erdős was ahead of this trend (and almost certainly contributed to it).

Erdős also stimulated mathematics by publicising his vast collection of problems; for many of them, he offered financial rewards for solutions. As an example, here is one of his most valuable problems. Let $A = \{a_1, a_2, \ldots\}$ be a set of positive integers with the property that the sum of the reciprocals of the members of A diverges. Is it true that A contains arbitrarily long arithmetic progressions? The motivating special case (for which the answer is not known) is that where A is the set of prime numbers: this is a problem in number theory, but Erdős' extension to an arbitrary set transforms it into combinatorics.

Increased collaboration among mathematicians goes beyond the influence of Erdős; combinatorics seems to lead the trend. Aspects of this trend include large international conferences (the Southeastern Conference on Combinatorics, Graph Theory and Computing, holding its 30th meeting in 1999, attracts over 500 people annually), and electronic journals (the *Electronic Journal of Combinatorics* [10], founded in 1994, was one of the first refereed specialist electronic journals in mathematics). Electronic publishing is particularly attractive to combinatorialists. Often, arguments require long case analysis, which editors of traditional print journals may be reluctant to include in full.

In wider terms, our time has seen a change in the scientific viewpoint from the continuous to the discrete. Two mathematical developments of the twentieth century (catastrophe theory and chaos theory) have shown how discrete effects can be produced by continuous causes. (Perhaps their dramatic names reflect the intellectual shock of this discovery.) But the trend is even more widespread.

In their book introducing a new branch of discrete mathematics (game theory), John von Neumann and Oskar Morgenstern [23] wrote:

> The emphasis on mathematical methods seems to be shifted more towards combinatorics and set theory – and away from the algorithm of differential equations which dominates mathematical physics.

How does discreteness arise in nature? Segerstråle [30] quotes John Maynard-Smith as saying "today we really do have a mathematics for thinking about complex systems and things which undergo transformations from quantity into quality" or from continuous to discrete, mentioning Hopf bifurcations as a mechanism for this.

On the importance of discreteness in nature, Steven Pinker [25] has no doubt. He wrote:

> It may not be a coincidence that the two systems in the universe that most impress us with their open-ended complex design – life and mind – are based on discrete combinatorial systems.

Here, 'mind' refers primarily to language, whose combinatorial structure is well described in Pinker's book. 'Life' refers to the genetic code, where DNA molecules can be regarded as words in an alphabet of four letters (the bases adenine, cytosine, guanine and thymine), and three-letter subwords encode amino acids, the building blocks of proteins.

The Human Genome Project was a major scientific enterprise to describe completely the genetic code of humans. (See [2] for an account of the mathematics involved.) At Pinker's university (the Massachusetts Institute of Technology), the Whitehead Laboratory was engaged in this project. Its director, Eric Lander, rounds off this chapter and illustrates its themes. His doctoral thesis [21] was in combinatorics, involving a 'modern' subject (coding theory), links within combinatorics (codes and designs), and links to other parts of mathematics (lattices and local fields). Furthermore, he is a fourth-generation academic descendant of Henry Whitehead.

References

[1] Kenneth Appel and Wolfgang Haken, Every planar map is four colorable, *Bulletin of the American Mathematical Society* **82** (1976), 711–712.

[2] Serafim Batzoglou, Bonnie Berger, Daniel J. Kleitman, Eric S. Lander and Lior Pachter, Recent developments in computational gene recognition, *Proceedings of the International Congress of Mathematicians*, Berlin 1998,

Documenta Mathematica special edition, available from
`http://www.mathematik.uni-bielefeld.de/documenta/xvol-icm/99/99.html`

[3] Joan S. Birman, The work of Vaughan F. R. Jones, in *Proceedings of the International Congress of Mathematicians,* Kyoto 1990, Mathematical Society of Japan/Springer-Verlag, Tokyo 1991, pp. 9-18.

[4] Joan S. Birman, Recent developments in braid and link theory, *Mathematical Intelligencer* **13** (1991), 52–60.

[5] Richard Borcherds, What is moonshine? *Proceedings of the International Congress of Mathematicians*, Berlin 1998, *Documenta Mathematica* special edition, available from
`http://www.mathematik.uni-bielefeld.de/documenta/xvol-icm/Fields/Fields.html`

[6] Jan Harrold Brunvald, *Too Good to be True: The Colossal Book of Urban Legends*, W. W. Norton, New York, 1999.

[7] F. E. Browder, Problems of present day mathematics, in *Mathematical Developments arising from Hilbert Problems*, Proceedings of Symposia in Pure Mathematics **28**, American Mathematical Society, Providence, 1976, pp. 35-79.

[8] Clay Mathematics Institute, press release 24 May 2000,
`http://www.claymath.org/prize_problems/PressStatement.htm`

[9] H. Crapo and G.-C. Rota, *On the Foundations of Combinatorial Theory: Combinatorial Geometries*, MIT Press, Cambridge, 1970.

[10] *Electronic Journal of Combinatorics*,
`http://www.combinatorics.org/`

[11] GAP homepage, `http://www-gap.dcs.st-and.ac.uk/~gap/`

[12] Kurt Gödel, Über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter Systeme, *Monatshefte für Mathematik und Physik* **38** (1931), 173–198. See also Gödel on the Net at
`http://www.sm.luth.se/~torkel/eget/godel.html`

[13] Daniel Gorenstein, *Finite Simple Groups: An Introduction to their Classification*, Plenum Press, New York, 1982.

[14] Jerrold W. Grossman, Paul Erdős: the master of collaboration, in *The Mathematics of Paul Erdős* (ed. R. L. Graham and J. Nešetřil), Springer-Verlag, Berlin, 1997, pp. 467–475. See also the Erdős Number Project website at
`http://www.oakland.edu/~grossman/erdoshp.html`

[15] M. Hall, Jr., and J. H. van Lint, *Combinatorics*, NATO ASI Series **C16**, D. Reidel, Dordrecht, 1975.

[16] Paul Hoffman, *The Man who Loved Only Numbers*, Hyperion, New York, 1998. See also the website for this book at
`http://www.paulerdos.com/`

[17] F. Jaeger, Strongly regular graphs and spin models for the Kauffman polynomial, *Geometriae Dedicata* **44** (1992), 23–52.

[18] Robert Kanigel, *The Man who Knew Infinity: A Life of the Genius Ramanujan*, Charles Scribner's Sons, New York, 1991.

[19] C. W. H. Lam, The search for a finite projective plane of order 10, *American Mathematical Monthly* **98** (1991), 305–318.

[20] C. W. H. Lam, S. Swiercz and L. Thiel, The nonexistence of finite projective planes of order 10, *Canadian Journal of Mathematics* **41** (1989), 1117–1123.

[21] E. S. Lander, *Topics in Algebraic Coding Theory*, D. Phil. thesis, Oxford University, 1980.

[22] Eugene M. Luks, Isomorphism of graphs of bounded valence can be tested in polynomial time, *Journal of Compututation and Systems Science* **25** (1982), 42–65.

[23] J. von Neumann and O. Morgenstern, *Theory of Games and Econmic Behavior*, Princeton University Press, Princeton, 1944.

[24] J. Paris and L. Harrington, A natural incompleteness in Peano arithmetic, in *Handbook of Mathematical Logic* (ed. Jon Barwise), North-Holland, Amsterdam, 1977, pp. 1133–1142.

[25] Steven Pinker, *The Language Instinct*, Penguin, London 1994.

[26] C. E. Praeger, Finite transitive permutation groups and finite vertex-transitive graphs, in *Graph Symmetry* (ed. G. Hahn and G. Sabidussi), Kluwer, Dordrecht, 1997, pp. 277–318.

[27] N. Robertson and P. D. Seymour, Graph minors, I: Excluding a forest, *Journal of Combinatorial Theory* (B) **35** (1983), 39–61, and subsequent papers with the same title.

[28] G.-C. Rota, On the foundations of combinatorial theory, I: Theory of Möbius functions, *Zeitschrift für Wahrscheinlichkeitstheorie* **2** (1964), 340–368.

[29] Bruce Schechter, *My Brain is Open: The Mathematical Journeys of Paul Erdős*, Simon & Schuster, New York, 1998.

[30] Ullica Segerstråle, *Defenders of the Truth: The Battle for Science in the Sociobiology Debate and Beyond*, Oxford University Press, Oxford, 2000.

[31] E. R. Swart, The philosophical implications of the four-color problem, *American Mathematical Monthly* **87** (1980), 697-707.

[32] Jacques Tits, *Buildings of Spherical Type and Finite BN-Pairs*, Lecture Notes in Mathematics **386**, Springer, Berlin, 1974.

[33] W. T. Tutte, *Graph Theory as I have Known it*, Oxford University Press, Oxford, 1998.

[34] W. T. Tutte, The coming of the matroids, in *Surveys in Combinatorics, 1999* (ed. J. D. Lamb and D. A. Preece), London Mathematical Society Lecture Notes **267**, Cambridge University Press, Cambridge, 1999, pp. 3–20.

[35] T. Tymoczko, Computers, proofs and mathematicians: a philosophical investigation of the four-color proof, *Mathematics Magazine* **53** (1980), 131-138.

[36] D. J. A. Welsh, *Complexity: Knots, Colourings and Counting*, London Mathematical Society Lecture Notes **186**, Cambridge University Press, Cambridge, 1993.