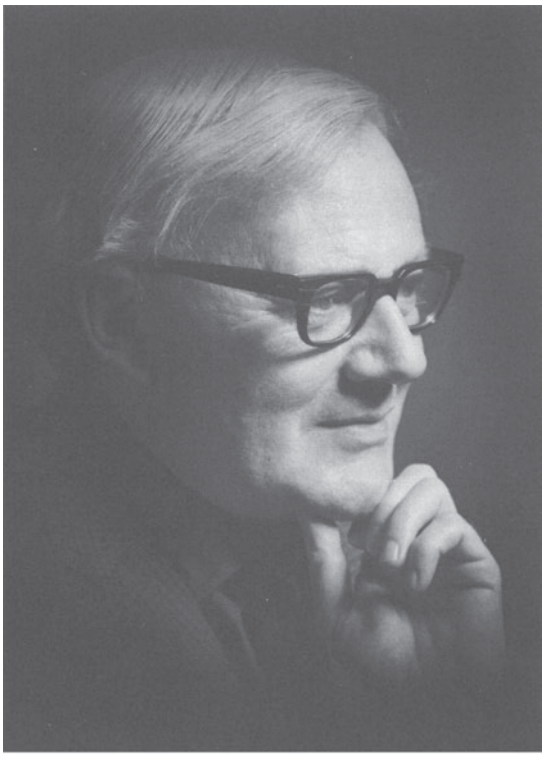
The Rado Lecture



Professor W. T. Tutte FRS

The Coming of the Matroids

W. T. Tutte

Summary The author rehearses his role in the development of the theory of matroids. The story starts in 1935 when he became an undergraduate at Trinity College, Cambridge, and started to collaborate with Leonard Brooks, Cedric Smith and Arthur Stone. It continues through his war-time work with codes and ciphers, followed by his return to Trinity in 1945, where his PhD thesis entitled "An Algebraic Theory of Graphs" foreshadowed his matroid papers published in 1958 and 1959. He describes the context in which he obtained the now well-known excluded minor conditions for a binary matroid to be regular and for a regular matroid to be graphic. He subsequently invented the whirl, and lectured on matroids at the 1964 Conference where the theory of matroids was first proclaimed to the world. This paper has two appendices: "Geometrical Terminology" and "Binary and Regular Matroids".

As we all know, matroids made their appearance in the mathematical literature in 1935, in a paper of Hassler Whitney entitled "On the abstract properties of linear dependence" [17].

Whitney looked at a matrix and saw that some sets of columns were independent and some were not. There were even simple rules about this distinction. For example, any subset of an independent set of columns is independent—provided of course that you count the null set as independent. Also, if you had an independent set A you could make it into a bigger one by adding the right member of any independent set that was bigger than A. In a flash of genius, Whitney said "Let us make these statements the axioms of a theoretical structure that is like a matrix and yet more than a matrix!"

I imagine him reflecting: "A spheroid is something like a sphere. A cycloid is something like a cycle. So something like a matrix could be a 'matroid'. So be it!"

Now Whitney, only a few years before, had published some important papers on graph theory—papers making up the nearest thing we had to a textbook on the subject [12–16]. Everyone knows nowadays that a graph has associated matroids, and it seems reasonable that matroid theory should develop out of graph theory. Whitney remarks on the connection between the two subjects in his introduction and carries over some terms from one theory to the other. That is why he calls a circuit a "circuit", though it does not always look like one.

But Whitney left graph theory, and perhaps matroid theory was the path by which he left—though we should note that having sojourned forty years in the wilderness he emerged to part-write a paper on the Four Colour Problem [18].

But let all that be introductory. I suppose you are not anxious for me to make this lecture a recitation from the literature. Better that I should tell

of experiences of my own, of how I myself encountered matroids and other abstractions from graph theory.

1935 was the year when I became an undergraduate at Trinity College, Cambridge. There I joined the Trinity Mathematical Society and formed an informal association with three other members, Leonard Brooks, Cedric Smith and Arthur Stone. The object of this association was the study of out-of-the-way mathematical problems, notably that of dissecting a square into unequal squares.

Since this problem depended on a knowledge of Kirchhoff's Laws for electric currents, it gave us an excellent grounding in graph theory. We therefore began to look at other graph-theoretical problems too.

Our association received different names from time to time. The Important Members, The Four Horsemen, The Gang of Four. Take your pick.

A set of currents in a graph obeying Kirchhoff's Laws we called a "Kirchhoff Chain". Arthur Stone, the topologist, pointed out that this chain was "a cycle modulo the poles" and "an absolute cocycle". Some years later, in a course on combinatorial topology, I found out what he meant.

Smith began to abstract from Four Colour Theory. He started with Tait's variation on that theory, which considers 3-colourings of the edges of a cubic graph G so that all three colours meet at each vertex. In Smith's first abstraction the edges of G became geometrical points associated in threes. Each triad of course corresponded to a vertex of G. He called his abstraction a "3-net".

Now if the edges of G are properly coloured in three colours a, b and c, then those of any two colours a and b form a "Tait cycle", that is, a union of one or more disjoint even circuits that takes in all the vertices. Smith now constructed a second 3-net that he called the "derivative" of the first. Its points were the Tait cycles—and they came in triads, one triad to each Tait colouring. Soon he had a derivative of the derivative, and so on [4].

I have told elsewhere [10] of how others of the Four watched apprehensively this process of abstraction and generalization. Soon Smith's 3-nets had become mere sets of points in a finite vector space, and a Tait colouring was an assignment to those points of non-zero members of the 4-group, the coefficients conforming to the linear relations of the points. It seemed to us other three that our beloved graph theory had vanished into a mist of algebra. "Graph theory" we would explain to our friends "is like the Cheshire cat: the cat has vanished but the grin remains".

Smith's 3-nets as I see them are not matroids but are based on the same principle. Generalize some aspect of graph theory; it shall undergo a change "Into something rich and strange".

I left Cambridge in 1941 with the idea that graph theory could be reduced to abstract algebra, but that it might not be the conventional kind of algebra.

There had been developments since 1935. The Four solved their problem about dissected squares. They wrote a paper about such dissections, eventually published in the Duke Mathematical Journal [1]. They researched on

Hamiltonian circuits. Then a war broke out. I found myself at Bletchley Park, in Buckinghamshire, studying some Continental codes and ciphers. (The work at Bletchley Park was part of the activities of GC & CS, the Government Code and Cipher School.)

I mention this because some of those ciphers posed problems that I thought involved a kind of linear algebra. We would receive an intercepted cipher message that was a long string of letters or teleprinter symbols. That could be called a vector. Call it C for "cipher". In the relevant cases C was formed from two other vectors, P for "plain language" and K for "key". We would have the simple equation

$$C = P + K$$

in some chosen finite arithmetic. The key K would be constructed on some secret machine.

There one had an equation in linear algebra and to start with we, in the Research Section at Bletchley, would know only C. Sometimes mistakes at the European end, such as sending two messages on the same key, would enable us to solve for K and the two P's [2].

In one case of importance, K was a sum of subkeys. Some of these were periodic, advancing one step for each letter. The others were basically periodic but for each new letter they sometimes advanced and sometimes stayed still. These subkeys each involved only two symbols, known to us as "dot" and "cross". The patterns of dot and cross were changed from time to time but the periods of the subkeys were fixed. We called the subkeys "wheels".

Sometimes, knowing C and assuming some statistical properties of P, we were able to disentangle the subkeys of K and determine them all, using a curious mixture of statistics and linear algebra. The problem would be simplified when we knew the cyclic patterns of the wheels and had thereafter only to determine their settings.

The point I want to make is that at Bletchley I was learning an odd new kind of linear algebra; I was still being prepared for the Coming of the Matroids.

I have been warned that this Conference is oriented towards Computer Science. That gives me another reason to mention Bletchley. For there an electronic computer was invented more than half a century ago.

I remember a particular problem of the time and place. We would have a sequence of dots and crosses, at least 2000 long, derived from a cipher message. We would have also a periodic sequence of dots and crosses, of period $31 \times 41 = 1271$, derived from our knowledge of the ciphering machine and its current wheel-patterns. We would want to compare the two in all their 1271 relative settings and pick the setting that gave the best agreement. If there was then a statistically significant agreement we would infer the setting of two wheels and go on to the next stage. Now 1271 comparisons per message were rather too many for the biological computers initially available, so electrical ones were invented and constructed, first with relays and then with thermionic valves (also called vacuum tubes) [2].

A replica of one of the later models can be seen now at Bletchley Park. Over and over again it finds the two sequences of dots and crosses, of periods 31 and 41, whose combination gives the best agreement with a long, long sequence derived from a genuine wartime cipher message.

Late in 1945 I found myself back at Trinity as a Fellow of the College. I now had to work for my PhD degree. What should be the subject of my thesis? Why not that abstractifying of graph theory in a reduction to linear algebra?

Following in the ways of Arthur Stone, I contemplated the additive group of cycles of a graph G, with coefficients in a ring R. Perhaps the coefficients would be integers as with our Kirchhoff chains. Perhaps they would be residues mod 2, as used for Tait cycles. Or perhaps even they would be elements of the four-group of 2-vectors mod 2. Such cycles in cubic graphs, with no zero coefficients, defined the Tait colourings. It seemed that many graph-theoretical entities could be described in terms of these additive cycle-groups.

Each cycle had its "support", the set of graph-edges with non-zero coefficients in it. It seemed good to define an elementary cycle as a non-zero cycle whose support contained that of no other non-zero cycle. That could be abbreviated as a "cycle with minimal (non-null) support". Those elementary cycles corresponded to the circuits of the graph. What a pleasing theorem!

Now I ventured to abstract after the manner of Smith. Forget the graph-structure. Replace it by a finite set S of objects called "cells". Giving a coefficient in R to each cell one got a "chain on S over R". A set of such chains, closed under addition and multiplication by elements of R, was a "chain-group". A cycle-group of a graph was merely a special case of a chain-group.

I went on happily developing a theory of chain-groups and their elementary chains, these latter of course being defined by minimal supports. The method was to select theorems about graphs and try to generalize them to chain-groups. These was not too difficult for theorems expressible in terms of circuits. But theorems about 1-factors imposed problems.

As I look back on this episode I am grieved to recall that I still did not appreciate the work of Whitney. Yet these chain-groups were half-way to matroids and their minimal supports were Whitney's matroid-circuits, his "minimal dependent sets". Perhaps if I had read, marked and learned that paper of Whitney's [17] I would have said "Look, Whitney has done this stuff better already; I will abandon chain-groups and write about other things". That, I think now, would have been a pity.

I understand that Richard Rado was once in a somewhat similar position writing about abstract linear dependence but unaware of the earlier work of Whitney. I get an urge of fellow-feeling with that great man to whom this lecture is dedicated. But my linear dependence was not yet abstract. It was still thoroughly and unadventurously orthodox.

Returning to my own story, I went on to a second stage in chain-group theory. I discussed "binary" chain-groups, those over the ring of residues

mod 2. Binary chain-groups have the interesting property that each chain is uniquely determined by its support. Then I wrote of "regular" chain-groups. These are over the ring of integers. But each elementary chain is restricted to the coefficients 0, 1 and -1, or is an integral multiple of such a chain of the group. An equivalent definition derives a regular chain-group from a totally unimodular matrix, that is, a matrix in which each square submatrix has determinant 1, -1 or 0. The chains correspond to the rows of the matrix and their linear combinations (with integral coefficients). Regular chain-groups were interesting because the cycle-group of a graph, over the integers, was always regular. Last came the "graphic" chain-groups, those that could be represented as integral cycle-groups of graphs.

The later part of my thesis established what would now be called "excluded minor" conditions first for a binary chain-group to be regularizable, that is, to correspond cell to cell and circuit to circuit with a regular chain-group, and then for a regular chain-group to be graphic [5]. All that foreshadowed my own contribution to matroid theory, published some ten years later [6–8].

In the interval I had my thesis accepted and received my PhD degree in 1948. I then became a lecturer at the University of Toronto. By 1958 I was an "Assistant Professor". In the interval I had learned to appreciate matroids. I put the work in my thesis into matroid terminology and generalized from chain-groups to matroids. I found conditions for a given matroid to be "binary", that is, the matroid of a binary chain-group. Then from the thesis-theorems I got the now well-known excluded minor conditions for a binary matroid to be regular and for a regular matroid to be graphic.

I published this work in a 2-part paper entitled "A homotopy theorem for matroids" [6, 7]. I do not find that homotopy theorem in the later literature. Perhaps it is mentioned with a warning that it is terribly long and then the author tells of some shorter, slicker proof of the excluded minor conditions. That is the way of Mathematics.

Yet I feel some sadness at the disappearance of the process of homotopy. It began with a geometrical representation of a matroid. The points were the circuits of a matroid, that is, its minimal dependent sets. To any set U of cells could be assigned a "rank", the least number of cells whose removal destroyed all the circuits in U. A union of circuits of rank 2 was a "line" and one of rank 3 was a "plane". And so on. With this terminology you could study matroid theory in a geometrical context provided you bore in mind that two points did not necessarily determine a line, nor three non-collinear points a plane. However two lines in a plane were conventional enough to intersect in a point.

There is a distinction between connected and disconnected lines. A disconnected line has two points only. And these, considered as circuits of the matroid, are disjoint. A connected line has three points. Since the theorem is about binary matroids there cannot be more than three points on a line.

Such combinatorial geometries are still met with. The homotopy paper went on to define a "linear subclass" as a set K of points which with any

two points on a connected line contained also the third. Then attention was directed to those re-entrant paths along the connected lines of the geometry that were "off K", that is, passed through no point of K. To me the most interesting part of the work described in the paper was showing that any such path could be reduced to a null path by a sequence of elementary operations of four kinds.

The first operation replaced

$$XYZYT \quad \text{by} \quad XYT \quad \text{or conversely.}$$

The second replaced

$$XYZTYU \quad \text{by} \quad XYU \quad \text{or conversely,}$$

provided that Y, Z and T were coplanar. The third replaced

$$XYZTUYV \quad \text{by} \quad XYV \quad \text{or conversely,}$$

provided that Y, Z, T and U were coplanar. There were two other points in the plane and these belonged to K.

The fourth operation uses a configuration that can be described briefly as projectively equivalent to a cube with its edges and faces extended to three points at infinity. Any two of these three make up a disconnected line. Four vertices of the cube, no two on the same edge, belong to C. An elementary path of the fourth kind is of the form $AXBYA$ where A and B are "points at infinity" and X and Y are distinct vertices of the cube not in C.

That was the homotopy theorem and I was able to use it to characterize regular matroids. The later result saying when a regular matroid was graphic was guided, in the usual vague graph-to-matroid way, by Kuratowski's Theorem and my favourite proof thereof [8].

One aspect of this work rather upset me. I had valued matroids as generalizations of graphs. All graph theory, I had supposed, would be derivable from matroid theory and so there would be no need to do independent graph theory any more. Yet what was this homotopy theorem, with its plucking of bits of circuit across elementary configurations, but a result in pure graph theory? Was I reducing matroid theory to graph theory in an attempt to do the opposite? Perhaps it was this jolt that diverted me from matroids back to graphs.

Yet I did do some more work on matroids. I can claim to have invented the whirl if not the wheel. And I lectured on matroids at the first formal conference devoted to them [4]. That conference was organised by Jack Edmonds and his colleagues at the National Bureau of Standards in Washington in 1964. To me that was the year of the Coming of the Matroids. Then and there the theory of matroids was proclaimed to the mathematical world. And outside the halls of lecture there arose the repeated cry: "What the hell is a matroid?" In their

text-books Dominic Welsh and James Oxley have attempted to answer that question [3, 11].

Richard Rado took a keen interest in abstract linear dependence, and his name is attached to an important theorem in the theory of transversals and transversal matroids [3, 11]. By the time I met him I was back with graphs and maps, trying to enumerate rooted planar maps of various kinds. My wife and I met Richard and Louise Rado quite often at Waterloo, at Reading and at conferences elsewhere. I enjoyed many stimulating conversations with him. When I spoke of my enumerative work he advised me earnestly to use exponential generating functions. Alas, I still have not found a way of doing that.

References

[1] R. L. Brooks, C. A. B. Smith, A. H. Stone & W. T. Tutte, The dissection of rectangles into squares, *Duke Mathematical Journal*, **7** (1940), 312–340.

[2] F. H. Hinsley and Alan Stripp, editors, *Codebreakers*, Oxford University Press (1993).

[3] J. G. Oxley, *Matroid Theory*, Oxford University Press (1992).

[4] C. A. B. Smith, Map colourings and linear mappings, in *Combinatorial Mathematics and its Applications, Proceedings of a Conference held at the Mathematical Institute, Oxford, from 7–10 July 1969*, (ed. D. J. A. Welsh), Academic Press, London (1969), pp. 259–283.

[5] W. T. Tutte, An Algebraic Theory of Graphs, PhD Thesis, Cambridge, 1948.

[6] W. T. Tutte, A homotopy theorem for matroids, I, *Transactions of the American Mathematical Society*, **88** (1958), 144–160.

[7] W. T. Tutte, A homotopy theorem for matroids, II, *Transactions of the American Mathematical Society*, **88** (1958), 161–174.

[8] W. T. Tutte, Matroids and Graphs, *Transactions of the American Mathematical Society*, **90** (1959), 527–552.

[9] W. T. Tutte, Lectures on Matroids, *Journal of Research of The National Bureau of Standards*, *Series B*, *Mathematics and Mathematical Physics*, **69B** (1965), 1–47.

[10] W. T. Tutte, *Graph Theory As I have Known It*, Oxford University Press (1998).

[11] D. J. A. Welsh, *Matroid Theory*, Academic Press, London (1976).

[12] H. Whitney, A theorem on graphs, *Annals of Mathematics 2*, **32** (1931), 378–390.

[13] H. Whitney, The colouring of graphs, *Annals of Mathematics 2*, **33** (1932), 688–718.

[14] H. Whitney, A logical expansion in mathematics, *Bulletin of the American Mathematical Society*, **38** (1932), 572–579.

[15] H. Whitney, 2-isomorphic graphs, *American Journal of Mathematics*, **55** (1933), 245–254.

[16] H. Whitney, Non-separable and planar graphs, *Transactions of the American Mathematical Society*, **34** (1932), 339–362.

[17] H. Whitney, On the abstract properties of linear dependence, *American Journal of Mathematics*, **57** (1935), 509–533.

[18] H. Whitney & W. T. Tutte, Kempe chains and the four colour problem, *Utilitas Mathematica*, **2** (1972), 241–281.

151 Manderston Road
Newmarket
Suffolk CB8 0NS