

9-1-2007

The Contributions of Dominic Welsh to Matroid Theory

James Oxley
Louisiana State University

Follow this and additional works at: https://repository.lsu.edu/mathematics_pubs

Recommended Citation

Oxley, J. (2007). The Contributions of Dominic Welsh to Matroid Theory. *Combinatorics, Complexity, and Chance: A Tribute to Dominic Welsh* <https://doi.org/10.1093/acprof:oso/9780198571278.003.0015>

This Article is brought to you for free and open access by the Department of Mathematics at LSU Scholarly Repository. It has been accepted for inclusion in Faculty Publications by an authorized administrator of LSU Scholarly Repository. For more information, please contact ir@lsu.edu.

THE CONTRIBUTIONS OF DOMINIC WELSH TO MATROID THEORY

JAMES OXLEY

ABSTRACT. Dominic Welsh began writing papers in matroid theory almost forty years ago. Since then, he has made numerous important contributions to the subject. His book *Matroid Theory* provided the first comprehensive treatment of the subject and has served as an invaluable reference to many workers in the field. Dominic's work on matroids has been characterized by his ability to build bridges between the subject and other areas of mathematics, by his talent for identifying tantalizing problems and making interesting conjectures that draw others in, by his infectious enthusiasm for problem solving that he has passed on to so many students, and by his writing on the subject that has popularized it making it both comprehensible and accessible. This paper reviews Dominic Welsh's work in and influence on the development of matroid theory.

1. INTRODUCTION

This year marks the seventieth anniversary of Whitney's founding paper in matroid theory [114]. The subject is now old enough to review its development and, in the present context, to describe the influence of Dominic Welsh on this development. There seem to be three notable groups of people that one can distinguish when discussing the development of matroid theory. First among these are the foundation layers, Whitney, of course, but also Birkhoff and Mac Lane. Their work and that of the other early contributors to matroid theory are reviewed in Joseph Kung's *A Source Book in Matroid Theory* [37]. The second group, the trailblazers, proved the major theorems in the subject. This group was led by Tutte, who was followed by Edmonds, then Seymour, and, very recently, by Geelen, Gerards, and Whittle. The third group, the bridge builders, consolidated the subject and developed its infrastructure by linking it to other areas of mathematics, by writing about it and thereby making it accessible to a broad audience, by challenging the workers inside and outside the area with tantalizing problems, and by infusing generations of students with enthusiasm for the subject. Two people stand out as clear leaders of the third group, the late Gian-Carlo Rota and

1991 *Mathematics Subject Classification.* 05B35.

The author was supported by the National Security Agency and by a Visiting Research Fellowship at Merton College, Oxford.

Dominic Welsh. This paper attempts to provide an overview of the many important contributions that Dominic Welsh has made to matroid theory.

After a brief burst of activity around the time of Whitney’s paper, matroid theory developed slowly until the late 1950s when Tutte published his important papers characterizing regular matroids [75] and graphic matroids [76]. There was a significant revival in the subject in the 1960s. Jack Edmonds organized the first conference in matroid theory at the National Bureau of Standards in 1965 and papers were presented there by, among others, Crapo, Edmonds himself, Nash-Williams, and Tutte. Henry Crapo was the first of a number of Ph.D. students of Rota who worked on *combinatorial geometries* (as Rota preferred to call matroids). Together Crapo and Rota wrote a matroid theory book in 1970 called *On the Foundations of Combinatorial Theory: Combinatorial Geometries* [14]. Dominic’s introduction to matroid theory came in 1966 in a “most stimulating seminar on the applications of matroid theory” [96, p. v] by Crispin Nash-Williams. Dominic’s book *Matroid Theory* [96] appeared a decade later. Essentially this survey will proceed chronologically through Dominic’s work distinguishing certain phases of concentration on particular topics. But there will be some historical discontinuities in the narrative because some of these topics have been recurring themes throughout Dominic’s career. A survey such as this inevitably reflects the bias of the author. An additional difficulty is posed by the fact that much of Dominic’s work touches on so many topics that it is difficult to classify as belonging to one area or another. It is hoped that, in spite of some omissions which particular readers may regret, this survey will do justice to the importance of Dominic’s work in matroid theory.

While many definitions will be given here, some basic ones will not. The terminology and notation used here will follow [55]. For a positive integer n , we shall use $[n]$ to denote the set $\{1, 2, \dots, n\}$.

2. MATROIDS VERSUS GRAPHS

Dominic was drawn into matroid theory through graph theory. The Oxford seminar by Nash-Williams where Dominic met matroids had shown how the matroid union operation could be used to give quick proofs of some covering and packing results for graphs whose original graph-theoretical proofs were quite intricate.

Several of Dominic’s earliest papers in matroid theory dealt with the links between graphs and matroids. He was one of a number of authors to independently discover that Kruskal’s theorem for graphs has a natural extension to matroids which produces a minimum-weight basis [87]. Curiously, the first to discover this seems to have been Borůvka [8] in 1926 nearly a decade before Whitney introduced matroids. In another paper [89], Dominic showed that the dual relationship that exists between Eulerian and bipartite graphs is a special case of a more general theorem for binary matroids. Specifically, he proved the following.

Theorem 2.1. *Let M be a binary matroid on a set E . Then every circuit of M has even cardinality if and only if M has a collection of disjoint cocircuits whose union is E .*

Dominic's book on matroids was written partially as a result of the urging of Frank Harary and together the two of them wrote a survey paper [27] in 1969 called "Matroids versus graphs". Its aim was to demonstrate to graph theorists "that matroid theory constitutes a natural generalization of graph theory" [27, p. 155]. This theme of linking matroids and graphs has been an important and recurrent one in Dominic's work just as it was in the work of another of the pioneers of matroid theory, Bill Tutte who, in the entry in *Mathematical Reviews* (MR0427112 (55#148)) for Dominic's book, wrote: "It has been said that to get a theorem on matroids we should take a known one on graphs, rewrite it and its proof so as to make no mention of vertices, and then replace the word "graph" by "matroid"." Dominic used this model in the paper with Harary when conjecturing an analogue of Dirac's Theorem [18] that a simple n -vertex graph in which every vertex has degree at least $\frac{n}{2}$ has a Hamiltonian cycle. The proposed matroid analogue of this was that a connected rank- r binary matroid in which every cocircuit has at least $\frac{1}{2}(r+1)$ elements has a spanning circuit. Although, much to Dominic's perpetual embarrassment, this conjecture fails for F_7^* , the dual of the Fano matroid, it does hold, for example, for all regular matroids. Indeed, Winfried Hochstättler and Bill Jackson [29] proved the following result. Observe that the hypotheses of the theorem do not require that the matroid be connected.

Theorem 2.2. *If M is a simple binary matroid that is not isomorphic to F_7^* and has no F_7 -minor, then M has a spanning circuit provided that every cocircuit of M has size at least $\max\{3, \frac{1}{2}(r+1)\}$.*

3. TRANSVERSAL THEORY

In the mid- to late 1960s, there were two identifiable centres of research into matroid theory in Britain: Oxford, where Dominic and Aubrey Ingleton worked, and Sheffield, where Leon Mirsky, Hazel Perfect, and John Pym were working. In Sheffield, the focus of the work was on transversal theory, that is, on Hall's Marriage Theorem and its generalizations. If (A_1, A_2, \dots, A_n) is a family \mathcal{A} of subsets of a finite set S , a *system of representatives* for \mathcal{A} is a sequence (e_1, e_2, \dots, e_n) such that $e_j \in A_j$ for all j in $[n]$. If e_1, e_2, \dots, e_n are distinct, then $\{e_1, e_2, \dots, e_n\}$ is a system of distinct representatives or a *transversal* of \mathcal{A} . The *partial transversals* of \mathcal{A} are the transversals of all the subfamilies of \mathcal{A} . Edmonds and Fulkerson [20] proved that this set of partial transversals forms the set of independent sets of a matroid on S , the *transversal matroid* $M[\mathcal{A}]$ of \mathcal{A} . This result was proved independently by Mirsky and Perfect [53], who also extended the result to infinite sets. In the same paper, Mirsky and Perfect drew attention to the

following result of Rado [61] whose significance had been previously overlooked. It is common in this work to denote a family of sets by $(A_i : i \in I)$ and, for $J \subseteq I$, to write $A(J)$ for $\cup_{j \in J} A_j$.

Theorem 3.1. *Let M be a matroid with rank function r and ground set S . A finite family $(A_i : i \in I)$ of subsets of S has a transversal that is independent in M if and only if*

$$r(A(J)) \geq |J| \text{ for all } J \subseteq I.$$

Dominic wrote a sequence of papers [88, 91, 92, 95] that presented various applications of this theorem of Rado. The highlight of this work appeared in a 1971 paper [95]. In that paper, Dominic proved an elegant theorem which, by using submodular functions, unified Hall's Marriage Theorem [25], Rado's Theorem stated above, and the defect versions of these theorems due to Ore [54] and Perfect (in [51]). The theorem was also powerful enough to imply a theorem of Hall on the existence of a system of common representatives for two families of sets [25], and a theorem of Rado (in [52]) giving necessary and sufficient conditions for a family of sets to have a system of representatives in which no element occurs more than k times. Dominic's theorem was obtained by extracting the essential features from a proof of Hall's Theorem due to Rado [62].

Theorem 3.2. *Let \mathcal{A} be a finite family $(A_i : i \in I)$ of subsets of a finite set S and let f be a non-negative, integer-valued function on 2^S such that*

- (i) *if $X \subseteq Y \subseteq E$, then $f(X) \leq f(Y)$; and*
- (ii) *if $X_1, X_2 \subseteq E$, then $f(X_1) + f(X_2) \geq f(X_1 \cup X_2) + f(X_1 \cap X_2)$.*

Then \mathcal{A} has a system of representatives $(e_i : i \in I)$ such that

$$f(\{e_j : j \in J\}) \geq |J| \text{ for all } J \subseteq I$$

if and only if

$$f(A(J)) \geq |J| \text{ for all } J \subseteq I.$$

Clearly Hall's Marriage Theorem and Rado's Theorem follow from the last result by taking f to be, respectively, the cardinality function on 2^S and the rank function r of M . Now let d be a non-negative integer not exceeding $|I|$. Then we obtain the following extension of Rado's Theorem, due to Perfect (in [51]), by letting $f(X) = r(X) - d$ for all $X \subseteq S$.

Corollary 3.3. *Let \mathcal{A} be a finite family $(A_i : i \in I)$ of subsets of a finite set S and let M be a matroid on S having rank function r . Then \mathcal{A} has a partial transversal that has size $|I| - d$ and is independent in M if and only if, for all subsets J of I ,*

$$r(A(J)) \geq |J| - d.$$

Dominic wrote two more papers on transversal matroids, one with his first student, Adrian Bondy, the other with his second student, Joan de Sousa. The paper with Bondy [6] included the following attractive theorem on presentations of transversal matroids.

Theorem 3.4. *Let \mathcal{A} be a family (A_1, A_2, \dots, A_n) of subsets of a finite set S and let M be the corresponding transversal matroid $M[\mathcal{A}]$. If $r(M) = r$, then there is a subset $\{j_1, j_2, \dots, j_r\}$ of $\{1, 2, \dots, n\}$ and a collection $C_1^*, C_2^*, \dots, C_r^*$ of distinct cocircuits of M such that $C_i^* \subseteq A_{j_i}$ for all i in $\{1, 2, \dots, r\}$ and M is the transversal matroid corresponding to the family $(C_1^*, C_2^*, \dots, C_r^*)$.*

The paper with Joan de Sousa [17] proves that a binary matroid is transversal if and only if it is graphic. When combined with a theorem of Bondy [5] and Las Vergnas [41], this yields the following result.

Theorem 3.5. *A binary matroid is transversal if and only if it has no minor isomorphic to $M(K_4)$.*

4. ENUMERATIVE PROBLEMS

In 1969, Dominic organized a conference in Oxford called “Combinatorial Mathematics and its Applications”. This conference is now recognized as the first British Combinatorial Conference. Dominic also organized what is now regarded as the third British Combinatorial Conference in 1972. These conferences continue today with the twentieth being held at Durham in July, 2005. The same theme that is so apparent in Dominic’s research of building bridges between combinatorics and other areas of mathematics is also apparent in his conference organization. The 1969 Oxford conference began with talks by Graham Higman on “Simple groups and combinatorial theory” and Mark Kac on “Some problems in statistical physics.” The conference included a talk by Roger Penrose entitled “Applications of negative dimensional tensors,” which, although it was opaque to many at the time, contained a wealth of interesting ideas that were subsequently generalized by various people including François Jaeger. This work was surveyed in 2001 by Martin Aigner [1].

Dominic’s presentation at that meeting [94] was called “Combinatorial problems in matroid theory”. It was a typical mixture of his problems. Some were solved by conference participants in time to appear in the conference proceedings, others were solved after a longer period including some quite recently, and still others remain unsolved acting as stimuli for current and future researchers. In two lectures given in Oxford in April and May, 2005, Dominic surveyed some of his favorites among these problems and we now consider several of these that are enumerative, beginning with three that remain unsolved. A sequence a_1, a_2, \dots, a_n is *unimodal* if there is a member m of $[n]$ such that $a_1 \leq a_2 \leq \dots \leq a_m$ and $a_m \geq a_{m+1} \geq \dots \geq a_n$. Let $f_k(n)$ be the number of rank- k non-isomorphic matroids on $[n]$. The following is Dominic’s Problem P19.

Problem 4.1. *Is the sequence $(f_k(n) : 0 \leq k \leq n)$ unimodal for all positive integers n ?*

Dominic's P20 was stated for even integers n . The next conjecture is the natural extension of this problem to all positive integers n .

Conjecture 4.2. *For all positive integers n , the maximum value of $f_k(n)$ occurs at $k = \lfloor \frac{n}{2} \rfloor$.*

For a non-negative integer k and a matroid M , let $i_k(M)$ be the number of k -element independent sets of M . The following is Dominic's Problem P13.

Conjecture 4.3. *For all matroids M , the sequence $(i_k : 0 \leq k \leq r(M))$ is unimodal.*

Three successive strengthenings of this conjecture were proposed by Mason [50]:

Conjecture 4.4. *If M is a matroid, then, for all k in $\{1, 2, \dots, r(M) - 1\}$:*

- (i) $i_k^2 \geq i_{k-1}i_{k+1}$;
- (ii) $i_k^2 \geq \binom{k+1}{k}i_{k-1}i_{k+1}$;
- (iii) $i_k^2 \geq \binom{k+1}{k} \left(\frac{i_1-k+1}{i_1-k} \right) i_{k-1}i_{k+1}$.

Progress on these conjectures has been very limited. Dowling [19] proved (i) for $k \leq 7$ and proposed a further extension of it; Hamidoune and Salaün [26] proved (iii) for $k = 3$ and conjectured another variant of it; Seymour [65] proved (iii) for those k such that M has no circuits of cardinality $3, 4, \dots$, or $k - 1$; and Mahoney [49] proved (i) when M is the cycle matroid of an outerplanar graph.

Two other enumerative problems from Dominic's list were solved quite recently after remaining open for over thirty years. Let $f(n)$ be the number of non-isomorphic matroids on an n -element set. The following theorem, which was proved independently by Lemos [47] and by Crapo and Schmitt [13], solves Dominic's Problem P22, which reproduced an earlier conjecture of his [90].

Theorem 4.5. *For all positive integers m and n ,*

$$f(m+n) \geq f(m)f(n).$$

Proof. Crapo and Schmitt's proof of this result is based on a new matroid operation that they introduce. For matroids M and N on disjoint sets, the *free product* $M \square N$ of M and N is the matroid on $E(M) \cup E(N)$ whose bases consist of those subsets of $E(M) \cup E(N)$ of size $r(M) + r(N)$ that consist of the union of an independent set in M and a spanning set in N . The theorem follows by showing that if $M \square N \cong P \square Q$, then M and N are isomorphic to P and Q , respectively. The reader is referred to Crapo and Schmitt's paper for the details. \square

Let $N_2(n)$ be the number of non-isomorphic binary matroids on an n -element set. Dominic's Problem P21 asked for the asymptotic behaviour of

$N_2(n)$. This problem has recently been solved by Marcel Wild although, as pointed out by Lax [46], Wild’s first paper on this topic [119] contained an error. A correction to that paper which proves a stronger result than the original paper is given in [120]. There is an interesting link here between matroid theory and linear codes.

A (linear) code of length n over $GF(q)$ is a subspace W of $V(n, q)$, the n -dimensional vector space over $GF(q)$. If W has dimension 0, then W consists of the zero vector of length n . If W has positive dimension r , then there is an $r \times n$ generator matrix D whose rows are linearly independent such that W equals the row space of D , the subspace of $V(n, q)$ that is spanned by the rows of D . Two codes W_1 and W_2 of length n over $GF(q)$ are (monomially) equivalent if there are a permutation σ of $\{1, 2, \dots, n\}$ and non-zero elements $\alpha_1, \alpha_2, \dots, \alpha_n$ of $GF(q)$ such that $(v_1, v_2, \dots, v_n) \in W_1$ if and only if $(\alpha_1 v_{\sigma(1)}, \alpha_2 v_{\sigma(2)}, \dots, \alpha_n v_{\sigma(n)}) \in W_2$. Evidently, W_1 and W_2 are equivalent if and only if one can obtain a generator matrix D_2 for W_2 from a generator matrix D_1 for W_1 by permuting the columns of the latter and then multiplying each column of the resulting matrix by a non-zero field element. Thus, if W_1 and W_2 are equivalent, then the matroids $M[D_1]$ and $M[D_2]$ are isomorphic. Although the converse of this is not true in general, it follows from the unique representability of binary and ternary matroids that the converse does hold when $q \in \{2, 3\}$ (see, for example, [55, Theorem 10.1.1]). Thus, for these two values of q , the number of inequivalent codes of length n over $GF(q)$ equals the number of non-isomorphic n -element $GF(q)$ -representable matroids.

For a prime power q and integers m and k with $0 \leq k \leq m$, the Gaussian coefficient $\begin{bmatrix} m \\ k \end{bmatrix}_q$ equals the number of k -dimensional subspaces of $V(m, q)$. It is well-known that

$$\begin{bmatrix} m \\ k \end{bmatrix}_q = \frac{(q^m - 1)(q^m - q) \cdots (q^m - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})}.$$

Evidently, $\frac{1}{n!} \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_2$ is the total number of subspaces of $V(n, 2)$. The following result was proved by Wild [120].

Theorem 4.6. *For all sufficiently large positive integers n ,*

$$\begin{aligned} (1 + 2^{-\frac{n}{2} + 2 \log_2 n + 0.2499}) \frac{1}{n!} \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_2 &\leq N_2(n) \\ &\leq (1 + 2^{-\frac{n}{2} + 2 \log_2 n + 0.2501}) \frac{1}{n!} \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_2. \end{aligned}$$

Hence

$$N_2(n) \sim \frac{1}{n!} \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_2.$$

Another proof of the asymptotic behaviour of $N_2(n)$ was given by Xiang-Dong Hou [31]. In a separate paper, Hou [30] verified a conjecture of Lax [46] by proving the following result.

Theorem 4.7. *The number of monomially inequivalent linear codes of length n over $GF(q)$ is asymptotic to $\frac{1}{n!(q-1)^{n-1}} \sum_{k=0}^n \binom{n}{k}_q$.*

Combining this theorem with the observations above about unique representability of ternary matroids, we immediately obtain the following result.

Corollary 4.8. *The number of non-isomorphic ternary matroids on an n -element set is asymptotic to $\frac{1}{n!2^{n-1}} \sum_{k=0}^n \binom{n}{k}_3$.*

The number $f(n)$ of non-isomorphic matroids on an n -element set occupied the attention of a number of researchers for about a decade from the mid-1960s. Crapo [11] proved that $f(n) \geq 2^n$. In one of his earliest papers, Dominic [90] considered the class of rank- r transversal matroids on $[n]$ having a *nested presentation*, that is, a presentation of the form $([i_1], [i_2], \dots, [i_r])$ where $1 \leq i_1 < i_2 < \dots < i_r \leq n$. Dominic proved that there are exactly $\binom{n}{r}$ non-isomorphic such transversal matroids. Summing this over all r in $\{0, 1, \dots, n\}$ gives that there are exactly 2^n non-isomorphic transversal matroids on $[n]$ having a nested presentation. It has only recently been noted (see Bonin, de Mier, Noy [7]) that this class of nested transversal matroids coincides with the class of matroids that Crapo used to obtain his lower bound. This lower bound was sharpened by Bollobás [4] in his only matroid paper to date. A significant improvement on these earlier bounds was obtained by Dominic [60] in a joint paper with his student, Mike Piff, where the following result was proved.

Theorem 4.9. *Let $g(n)$ be the number of non-isomorphic simple matroids on an n -element set. Then*

$$\log_2 \log_2 g(n) \geq n - \frac{5}{2} \log_2 n + O(\log \log n).$$

Subsequently, Knuth [36] improved this lower bound, replacing $\frac{5}{2}$ by $\frac{3}{2}$, and Piff [58] proved what is still the best-known upper bound on $f(n)$:

$$\log_2 \log_2 f(n) \leq n - \log_2 n + O(\log \log n).$$

5. THE TUTTE POLYNOMIAL AND GENERALIZATIONS OF IT

Probably the most important polynomial in graph theory or matroid theory is the Tutte polynomial, and work on this and related polynomials has been one of the most dominant themes in Dominic's research since the early 1970s. For a graph G , let $b(G)$ denote the number of spanning trees of G . In a joint paper with Brooks, Smith, and Stone, Tutte [9] noted a formula that implies that, for all non-loop edges e of G ,

$$(1) \quad b(G) = b(G \setminus e) + b(G/e).$$

Tutte wrote [81, p.53]: “When I was doing my Ph.D. research I began to collect other functions of graphs that satisfied similar recursions.” For a graph G and a positive integer λ , let $P(G; \lambda)$ be the number of colorings of the vertices of G using $\{1, 2, \dots, \lambda\}$ such that if two vertices are joined by an edge, they receive different colors. George D. Birkhoff [3] introduced $P(G; \lambda)$ in 1912–13 and R.M. Foster (in [113]) made the elementary observation that if e is an edge of G , then

$$(2) \quad P(G; \lambda) = P(G \setminus e; \lambda) - P(G/e; \lambda).$$

Using this, it is easily shown that the function P is a polynomial in λ ; it is called the *chromatic polynomial* of G .

Now orient the edges of G arbitrarily and let H be an abelian group. An H -flow on G is an assignment of non-zero members of H to the edges of G such that, at every vertex, the total flow into the vertex equals the total flow out from the vertex, where all calculations are done in H . Tutte showed that the number of such H -flows depends not on the specific group H but only on the order of H . In particular, if $|H| = m$, then the number of H -flows equals the number of \mathbb{Z}_m -flows. We call the latter flows m -flows and let $F(G; m)$ be the number of such flows. Tutte showed that

$$(3) \quad F(G; m) = F(G/e; m) - F(G \setminus e; m).$$

The polynomial F is called the *flow polynomial* of G .

These observations led Tutte to discuss a function f on graphs that is invariant under isomorphism:

$$(4) \quad f(G_1) = f(G_2) \text{ if } G_1 \cong G_2;$$

and satisfies the rule,

$$(5) \quad f(G) = f(G \setminus e) + f(G/e) \text{ for all non-loop edges } e \text{ of } G.$$

He also considered functions satisfying the additional condition that

$$(6) \quad f(H + K) = f(H)f(K)$$

where $H + K$ is the graph that is the union of the disjoint graphs H and K . Tutte proved that a graph function satisfying (4)–(6) is uniquely determined once its value is known, for all k , on the graphs consisting of a single vertex and k loops.

Tutte also introduced a 2-variable polynomial, which he called the *dichromate* and which is now known as the *Tutte polynomial*. This polynomial satisfies (5) provided e is not a bridge of G . It also satisfies (4) and (6) and, indeed, it is the universal graph invariant satisfying these three conditions in a sense that will shortly be made precise. The dichromate is frequently confused with the *dichromatic polynomial*, a different polynomial also introduced by Tutte. The precise relationship between these polynomials is discussed by Farr [21, Section 3] elsewhere in this volume.

Much of the theory described above extends to matroids and was developed by Tutte for representable matroids in his 1948 Cambridge Ph.D. thesis

[73]. However, Tutte never published his work for matroids and it was not until 1969 that Crapo [12] published a fully general matroid form of this theory. For a matroid M on a set E , the *Tutte polynomial* $T(M; x, y)$ of M is

$$\sum_{A \subseteq E} (x-1)^{r(E)-r(A)} (y-1)^{|A|-r(A)}.$$

This polynomial has the attractive property that

$$T(M; x, y) = T(M^*; y, x),$$

where M^* is the dual of the matroid M . Moreover, for a graph G with $k(G)$ components,

$$P(G; \lambda) = \lambda^{k(G)} (-1)^{|V(G)|-k(G)} T(M(G); 1-\lambda, 0)$$

and

$$f(G; m) = (-1)^{|E(G)|-|V(G)|+k(G)} T(M(G); 0, 1-m).$$

The Tutte polynomial has the properties that

$$(7) \quad f(M_1) = f(M_2) \text{ if } M_1 \cong M_2;$$

$$(8) \quad f(M) = f(M \setminus e) + f(M/e) \text{ if } e \text{ is not a loop in } M \text{ or } M^*;$$

and

$$(9) \quad f(M) = f(M \setminus e) f(M \setminus (E(M) - \{e\})) \text{ if } e \text{ is a loop of } M \text{ or } M^*.$$

In his thesis [73], Tutte showed that the Tutte polynomial is a universal matroid invariant satisfying (7)–(9) in that if the value of f on the two one-element matroids, $U_{1,1}$ and $U_{0,1}$, are x and y , respectively, then $f(M) = T(M; x, y)$ for all matroids M . Tutte never published this result for matroids although, for graphs, it is implicit in one of his papers [78]. The result for matroids was rediscovered by Brylawski [10] and published in 1972. In a joint paper with the author [56], Dominic extended this result to prove what he calls a “recipe theorem” for invariants of this type.

Theorem 5.1. *Let \mathcal{M} be a class of matroids that is closed under isomorphisms, direct sums, and taking minors, and contains both $U_{1,1}$ and $U_{0,1}$. Let g be an isomorphism invariant that maps the members of \mathcal{M} into a field \mathbb{F} and has the following properties for some fixed σ and τ in \mathbb{F} :*

- (i) *if $M \in \mathcal{M}$ and e is an element of M that is neither a loop nor a coloop of M , then $g(M) = \sigma g(M \setminus e) + \tau g(M/e)$; and*
- (ii) *if M_1 and M_2 are members of \mathcal{M} having disjoint ground sets, then $g(M_1 \oplus M_2) = g(M_1)g(M_2)$.*

Then, for all matroids M ,

$$g(M) = \sigma^{|E|-r(E)} \tau^{r(E)} T(M; \frac{x_0}{\tau}, \frac{y_0}{\sigma})$$

where x_0 and y_0 are the values that g takes on $U_{1,1}$ and $U_{0,1}$, respectively.

As an example of an application of this theorem [56], suppose that every element of a matroid M on a set E has, independently of all other elements, a probability $1 - p$ of being deleted from M . The resulting restriction $\omega(M)$ of M is a *random submatroid* of M corresponding in the obvious way to a random graph on n vertices when M is the cycle matroid of K_n . If we let $Pr(M)$ be the probability that $\omega(M)$ has the same rank as M , then, evidently, $Pr(U_{1,1}) = p$ and $Pr(U_{0,1}) = 1$. Moreover, if e is neither a loop nor a coloop of M , then $Pr(M) = (1 - p)Pr(M \setminus e) + pPr(M/e)$ and $Pr(M_1 \oplus M_2) = Pr(M_1)Pr(M_2)$. Hence

$$Pr(M) = (1 - p)^{|E|-r(E)} p^{r(E)} T(M; 1, \frac{1}{1-p}).$$

Thus, for instance, if $p = \frac{1}{2}$, then

$$Pr(M) = \frac{T(M; 1, 2)}{2^{|E|}}.$$

But $T(M; 1, 2)$ is easily seen to be the number of spanning sets of M . Hence, as one would expect, $Pr(M)$ is the probability that a randomly chosen subset of E spans M .

This recipe theorem has numerous other applications and it has served as a model for similar theorems describing more general matroid invariants. If $b_k(G; \lambda)$ is the number of vertex colourings of a graph G with λ colours in which exactly k edges have ends the same colour, then

$$b_k(G; \lambda) = b_k(G \setminus e; \lambda) - b_{k-1}(G/e; \lambda) + b_{k-1}(G/e; \lambda).$$

Dominic and Geoff Whittle [108] developed a theory of functions obeying such a 3-term recurrence and proved a recipe theorem for them. This theory has applications to channel assignments, subspace arrangements, hypergraph colourings, and counting lattice points.

In a joint paper with Koko Kayibi [107], Dominic introduced a 4-variable polynomial $Q(M, N; x, y, u, v)$ that is defined for matroids M and N with a common ground set E and rank functions r and s by

$$\sum_{X \subseteq E} (x - 1)^{r(E)-r(X)} (y - 1)^{|X|-r(X)} (u - 1)^{s(E)-s(X)} (v - 1)^{|X|-s(X)}.$$

Thus, for example, $Q(M, N; x, y, 2, 2) = T(M; x, y)$. Michel Las Vergnas has noted [45] that the 4-variable polynomial Q is actually equivalent to a 3-variable polynomial introduced by Las Vergnas himself [42, 43, 44] and defined for a *matroid perspective* (M_1, M_2) , that is, a pair of matroids, M_1 and M_2 , on a common ground set E such that the identity map on E is a *strong map*, taking every circuit of M_1 to a union of circuits of M_2 .

Evidently, Q has as evaluations all of the well-known evaluations of the Tutte polynomial of M such as the numbers of bases, independent sets, and spanning sets of M . In addition, as Dominic and Koko observe, $Q(M, N; 1, 1, 1, 1)$ and $Q(M, N; 2, 1, 2, 1)$ equal, respectively, the number of common bases of M and N and the number of common independent sets of

M and N ; and the specializations of Q include not only the Tutte polynomials of M and N , but also Oxley and Whittle’s rank generating function [57] of a 2-polymatroid f in the case when f is $r + s$.

The polynomial Q shares many of the properties of the Tutte polynomial. In particular, $Q(M^*, N^*; x, y, u, v) = Q(M, N; y, x, v, u)$. Moreover, Q satisfies nine different deletion-contraction formulae depending on whether the element e is a loop, a coloop, or neither in M , and a loop, a coloop, or neither in N . The main result of [107] extends the recipe theorem for the Tutte polynomial to Q . In particular, it is proved that if $\psi(M, N)$ is a function satisfying weighted versions of the nine deletion-contraction formulae, then, provided $\psi(U_{1,1}, U_{1,1})\psi(U_{0,1}, U_{0,1}) \neq \psi(U_{1,1}, U_{0,1})\psi(U_{0,1}, U_{1,1})$, the function ψ is a weighted evaluation of the polynomial Q .

6. COLOURINGS, FLOWS, AND THE CRITICAL PROBLEM

In the late 1970s and early 1980s, Dominic became very interested in “the use of matroids to relate problems about colourings and flows in graphs with problems in projective geometry” [97]. In 1954, Tutte [74] made two interesting conjectures for flows. The first, which was settled by Jaeger [32] in 1976, asserted that there is a fixed integer n such that every graph without a bridge has an n -flow. Jaeger proved that every such graph has an 8-flow and, subsequently, Seymour [67] proved that it has a 6-flow. Tutte’s second conjecture, the 5-Flow Conjecture, is that every bridgeless graph has a 5-flow. The *Petersen graph* P_{10} , which can be obtained from the dodecahedron by identifying antipodal vertices and then replacing each pair of parallel edges by a single edge, has no 4-flow, so 5 is best-possible in Tutte’s conjecture.

In his 1966 paper “On the algebraic theory of graph colorings” [77] following a suggestion of O. Veblen, Tutte developed a “geometrical version of the Four Color Problem” [79]. These ideas were further developed by Crapo and Rota [14] as part of their “critical problem” for matroids, a framework which encompasses a large family of extremal problems, including the 5-Flow Conjecture and the Four Colour Problem. Rota [64] defined the characteristic polynomial for a family of partially ordered sets that includes geometric lattices. Since the latter coincide with the lattices of flats of matroids, this leads to the following definition of the *characteristic polynomial* $P(M; \lambda)$ of a matroid M on a set E :

$$P(M; \lambda) = \sum_{X \subseteq E} (-1)^{|A|} \lambda^{r(E) - r(A)}.$$

Dominic calls $P(M; \lambda)$ the *chromatic polynomial* of M since if $M = M(G)$ for a loopless graph G having $k(G)$ components, then $P(G; \lambda) = \lambda^{k(G)} P(M(G); \lambda)$ and $F(G; \lambda) = P(M^*(G); \lambda)$. In general, $P(M; \lambda) = (-1)^{r(M)} T(M; 1 - \lambda, 0)$.

Crapo and Rota [14] proved the following attractive result.

Theorem 6.1. *Let M be a loopless $GF(q)$ -representable matroid of rank r and φ be a rank-preserving mapping from $E(M)$ into $E(PG(r-1, q))$. Then the rank of the largest subspace of $PG(r-1, q)$ avoiding $\varphi(E(M))$ is $r-c(M; q)$ for some fixed integer $c(M; q)$ that is independent of φ . Moreover, $c(M; q)$ is the least positive integer j such that $P(M; q^j) > 0$.*

The number $c(M; q)$ is called the *critical exponent* of M over $GF(q)$. In particular, $c(PG(r-1, q); q) = r$, so $c(F_7; 2) = 3$. Moreover, the critical exponent can be thought of as an analogue of the chromatic number $\chi(G)$ of a graph G for, if $M = M(G)$, then

$$q^{c(M; q)-1} < \chi(G) \leq q^{c(M; q)}.$$

In particular, $c(M(K_5); 2) = 3$.

Hadwiger's famous conjecture [24] for graphs can be stated as follows.

Conjecture 6.2. *For all positive integers m , the unique graph with chromatic number m for which every loopless proper minor has chromatic number less than m is K_m .*

Tutte's geometrical version of the Four Colour Problem is the following.

Conjecture 6.3. *The only binary matroids with critical exponent 3 for which every proper loopless minor has critical exponent less than 3 are $M(K_5)$, F_7 , and $M^*(P_{10})$.*

This conjecture is known as Tutte's Tangential 2-Block Conjecture as a matroid M that is representable over $GF(q)$ and has critical exponent exceeding k is a *tangential k -block over $GF(q)$* if every loopless non-empty proper minor of M has critical exponent at most k . From above, it is straightforward to deduce that each of $M(K_5)$ and F_7 is a tangential 2-block over $GF(2)$ and that $c(M^*(P_{10}); 2) = 3$. Tutte proved his conjecture [77] for tangential 2-blocks of rank at most 6, and B. T. Datta [15, 16] proved that there are no binary tangential 2-blocks of rank 7 or 8. The most significant advance towards the resolution of this conjecture was made in 1981 by Seymour [68], who proved the following result.

Theorem 6.4. *A binary tangential 2-block is either $M(K_5)$ or F_7 , or it is the dual of a graphic matroid.*

The proof of this result uses some very difficult results including what had then become the Four Colour Theorem of Appel and Haken [2] and Seymour's own decomposition theorem for regular matroids [66]. A consequence of Theorem 6.4 is that Tutte's Tangential 2-Block Conjecture is equivalent to the following extension of the 5-Flow Conjecture known as the 4-Flow Conjecture.

Conjecture 6.5. *Suppose that a graph G without bridges has no 4-flow. Then G has a subgraph contractible to P_{10} .*

Although this conjecture remains open in general, Robertson, Sanders, Seymour, and Thomas (in [71]) settled it in the important special case when G is a cubic graph.

In joint work with his student Paul Walton [85], Dominic proved the following result.

Theorem 6.6. *The only tangential 1-blocks over $GF(3)$ are $M(K_4)$ and $U_{2,4}$.*

Dominic gave a plenary lecture at the 1979 Dutch Mathematical Congress and the survey paper published in connection with that lecture [98] contained a number of conjectures on tangential k -blocks which, at the time, seemed very scarce. In a sequence of four papers [115, 116, 117, 118], Geoff Whittle presented a family of examples showing that this is not the case. Indeed, a consequence of [116] is that there are rank- r tangential blocks over $GF(q)$ for all r such that $k + 1 \leq r \leq q^k$. Whittle used the complete principal truncation [115] and then the more general quotient operation [116] to construct new tangential k -blocks from existing ones. He also showed how jointless Dowling geometries can be tangential k -blocks [118]. Perhaps the simplest of his constructions is that of a q -lift [117]. Suppose that M is a simple rank- r matroid that is representable over $GF(q)$. Then there is a subset X of $PG(r, q)$ such that $PG(r, q)|X \cong M$. Evidently X spans a hyperplane H of $PG(r, q)$. Take a point p of $PG(r, q)$ that is not in H . Let M' be the restriction of $PG(r, q)$ to the union of all lines of the latter that contain p and some point of X . The matroid M' is called a q -lift of M and Whittle [117] proved the following result.

Theorem 6.7. *If M is a tangential k -block over $GF(q)$ and M' is a q -lift of M , then M' is a tangential $(k + 1)$ -block over $GF(q)$.*

The constructions presented by Whittle show that tangential blocks are very geometrical in nature and the intuition that one gets about them from graphs can be very misleading. An interesting survey of critical problems for matroids by Kung [40] includes a comprehensive treatment of known results on tangential blocks. That paper includes the following attractive result.

Theorem 6.8. *Let M be a simple rank- r matroid that is representable over $GF(q)$ and M' be a q -lift of M . Then*

$$P(M'; \lambda) = (\lambda - 1)q^r P(M; \frac{\lambda}{q}).$$

Kung's paper concludes with the following interesting conjecture, which is very much in the spirit of a number of problems that are of central interest in matroid theory at present.

Conjecture 6.9. *For all prime powers q and all positive integers k , there are only finitely many tangential k -blocks over $GF(q)$.*

The chromatic number of a loopless graph G is the first positive integer j for which $P(G; j)$ is positive. Of course, this coincides with the first positive

integer k for which $P(G; m)$ is positive for all integers m with $m \geq k$. For matroids the situation is more complicated. For example, $P(F_7; \lambda) = (\lambda - 1)(\lambda - 2)(\lambda - 4)$ so $P(F_7 \oplus F_7; \lambda) = (\lambda - 1)^2(\lambda - 2)^2(\lambda - 4)^2$. Hence $P(F_7 \oplus F_7; \lambda)$ is positive for λ equal to three, zero for λ equal to four, and positive for each larger integer. For a loopless matroid M , let $\pi(M)$ be the least positive integer k for which $P(M; m)$ is positive for all integers $m \geq k$. By a theorem of Lindström [48], if M is regular, then

$$\pi(M) = \min\{j \in \mathbb{Z}^+ : P(M; j) > 0\}.$$

But, for matroids in general, the left-hand side here can exceed the right-hand side by an arbitrarily large number.

In another paper with Walton [84], Dominic considered bounding $\pi(M)$ for loopless binary matroids having certain excluded minors. For a collection M_1, M_2, \dots, M_k of matroids, let $EX(M_1, M_2, \dots, M_k)$ be the class of matroids having no minor isomorphic to any of M_1, M_2, \dots, M_k . For a class \mathcal{M} of matroids, let $\pi(\mathcal{M}) = \max\{\pi(M) : M \in \mathcal{M}\}$ if this maximum exists, and let $\pi(\mathcal{M})$ be ∞ otherwise. The Four Colour Theorem can be restated as

$$\pi(EX(U_{2,4}, F_7, F_7^*, M(K_5), M^*(K_5), M(K_{3,3}), M^*(K_{3,3})) = 4.$$

Wagner's theorem [86] establishing the equivalence of Hadwiger's conjecture for $n = 5$ and the Four Colour Theorem means that the last equation can be strengthened to

$$\pi(EX(U_{2,4}, F_7, F_7^*, M(K_5), M^*(K_5), M^*(K_{3,3})) = 4.$$

The next two theorems are from [84].

- Theorem 6.10.** (a) $\pi(EX(U_{2,4}, F_7, M(K_5), M^*(K_{3,3})) = 4.$
 (b) $\pi(EX(U_{2,4}, F_7^*, M(K_5), M^*(K_{3,3})) = 5.$
 (c) $\pi(EX(U_{2,4}, F_7, M(K_{3,3}), M^*(K_{3,3})) = 5.$
 (d) $\pi(EX(U_{2,4}, F_7^*, M(K_{3,3}), M^*(K_{3,3})) = 5.$

Theorem 6.11. *Tutte's 5-Flow Conjecture is equivalent to each of the following statements.*

- (a) $\pi(EX(U_{2,4}, F_7, M(K_5))) = 5.$
 (b) $\pi(EX(U_{2,4}, F_7^*, M(K_5))) = 5.$
 (c) $\pi(EX(U_{2,4}, F_7, M(K_{3,3}))) = 5.$
 (d) $\pi(EX(U_{2,4}, F_7^*, M(K_{3,3}))) = 5.$

That paper also shows, using Jaeger's 8-Flow Theorem that, for example, $\pi(EX(U_{2,4}, F_7, M(K_5))) \leq 8$. The proof technique used there, when combined with Seymour's 6-Flow Theorem implies that $\pi(EX(U_{2,4}, F_7, M(K_5))) \leq 6$, and (b)–(d) from the last theorem can be similarly modified to give true statements. It is also noted in that paper that no example is known to contradict the statement that $\pi(EX(U_{2,4}, M(K_5))) \leq 8$. Indeed, Dominic made the following interesting conjecture [98]:

$$\pi(EX(U_{2,4}, M(K_5))) \leq 5.$$

Using an intricate argument, Kung [38] proved in 1987 that

$$\pi(EX(U_{2,4}, M(K_5))) \leq 2^8,$$

but there seems to have been no further progress on this problem.

7. THE BOOK AND OTHER EXPOSITORY WRITING

Dominic's book *Matroid Theory* [96] appeared in 1976 with the stated aim of showing “the unifying and central role which matroids have played in combinatorial theory over the past decade” [96, p. v]. That decade is probably the most active that had ever occurred in the subject. There had been earlier books, by Crapo and Rota [14] in 1970 and by Tutte [80] in 1971, but neither of these was as comprehensive in its treatment of the subject, and the first only ever appeared in a preliminary edition. The three-volume series edited by Neil White [110, 111, 112], a former student of Rota, was conceived partially as a final version of the Crapo and Rota book. Dominic's book became the standard reference in the area. It succeeded in its goals of showing how “many parts of graph theory, transversal theory, block designs and combinatorial lattice theory can be more clearly understood by the use of matroids” [96, p. v]. It also indicated well how matroids “serve as a link between combinatorics and the more mainstream areas of mathematics” [96, p. v]. When I wrote my own book on matroids [55] in 1992, I did so only after Dominic had declined an offer from Oxford University Press to update his book. Indeed, when I was writing my book, Dominic's book was an invaluable organizational template for me.

Dominic has gone on to write books in a number of other areas of combinatorics and probability [23, 100, 102, 69] and he has also edited conference proceedings [93, 109]. In matroid theory, he has continued to make very important contributions through a series of survey papers, several of which have already been mentioned [27, 94, 97, 98, 99, 101, 103, 104, 105, 106]. These papers have become a hallmark of Dominic's career. He identifies interesting problems, frequently linking apparently disparate areas of mathematics, and then presents very readable accounts of the problems that entice others into considering them. He is very skilled at stripping away the technicalities to expose the core of a problem; and he is not embarrassed to make bold conjectures recognizing that the inherent challenge raised by a conjecture makes it more compelling than a problem. By posing conjectures, Dominic draws people into an area knowing that the failure of a plausible conjecture does much to reveal the complexities of the landscape surrounding a problem.

8. THE TUTTE POLYNOMIAL AND COMPLEXITY

In an important paper [34] with his student Dirk Vertigan and Jaeger, Dominic considered the complexity of evaluating the Tutte polynomial at particular points of the (x, y) -plane. This paper marks the beginning of an intensive study by Dominic of complexity issues relating to the Tutte

polynomial, which has occupied much of his attention for the last fifteen years. The original motivation for the paper with Jaeger and Vertigan was to determine whether or not calculating the Jones polynomial of a link [35] is a feasible computation. At the time, it was known that the Alexander-Conway polynomial of a link, being an evaluation of a determinant, could be determined in polynomial time. But Jaeger [33] and Thistlethwaite [70], respectively, had shown that computing the HOMFLY and Kauffman polynomials of a link are NP -hard. Since the Jones polynomial is a 1-variable specialization of each of the last two polynomials, the issue of determining its complexity was a natural one. Further, since the Jones polynomial of an *alternating* link, one whose crossings alternate between under and over, is, up to an easily derived factor, a specialization of the Tutte polynomial of an associated planar graph, it was also natural to consider the complexity of evaluating $T(M; x, y)$. The main result of [34] is that, except when (x, y) is one of a small number of special points or lies on a special hyperbola, calculation of $T(M; x, y)$ for a matroid M is $\#P$ -hard.

A formal description of the class $\#P$ can be found in Garey and Johnson [22]. Informally, Jaeger, Vertigan, and Welsh [34] described $\#P$ as the class of enumeration problems in which the structures being counted are recognizable in polynomial time, that is, there is an algorithm that, in time polynomial in the size of the problem instance, will verify whether a given structure has the correct form to be included in the count. A problem A in $\#P$ is $\#P$ -complete if, for every B in $\#P$, the problem B is polynomial-time reducible to A . An example of such a problem is counting the number of Hamiltonian paths in a graph. A problem is $\#P$ -hard if some $\#P$ -complete problem is polynomial-time reducible to it.

Because the number of matroids on an n -element set is so large, to specify such a matroid, the natural input size is $O(2^n)$. But, using the usual deletion-contraction formula for the Tutte polynomial enables it to be calculated in $O(2^n)$. The results in [34] concern matroids that have relatively compact descriptions using, say, a graph or a matrix. Formally, a class \mathcal{M} of matroids is *succinct* if there is an encoding of the members of \mathcal{M} into strings from some finite alphabet such that there is a polynomial p so that the length of the encoding of an n -element member of \mathcal{M} is at most $p(n)$. Three particular problems are considered in [34]. In the standard format of complexity theory, the first is:

$\pi_1[\mathcal{M}]$: \mathcal{M} -TUTTE POLYNOMIAL

Instance: matroid M belonging to a succinct class \mathcal{M} .

Output: the Tutte polynomial of M .

The question is also considered of evaluating the Tutte polynomial at a particular point or along particular curves in the (x, y) plane. Here one runs into issues about the field \mathbb{F} in which the calculations are done, with this field needing to be countable. Assume that \mathbb{F} is a finite-dimensional algebraic extension of the rationals and that \mathbb{F} contains the complex numbers i and

j where $j = e^{2\pi i/3}$. The problem of evaluating the Tutte polynomial at a point (a, b) where both a and b are in \mathbb{F} can now be precisely formulated:

$\pi_2[\mathcal{M}, a, b]$: \mathcal{M} -TUTTE POLYNOMIAL EVALUATION at (a, b)

Instance: matroid M belonging to a succinct class \mathcal{M} .

Output: $T(M; a, b)$.

For the problem of evaluating the Tutte polynomial along a curve L in the (x, y) -plane, attention is restricted to the case when L is a rational curve, that is, the set of points parameterized in standard form by

$$x(s) = \frac{u(s)}{v(s)}, y(s) = \frac{w(s)}{z(s)},$$

where u, v, w, z are given polynomials in $\mathbb{F}(s)$; a rational function is in *standard form* if the numerator and denominator are relatively prime and the denominator has leading coefficient one. Euclid's algorithm can be used to put a rational function in standard form in polynomial time. Along L , the Tutte polynomial of M is a rational function of s . Thus the following computational problem is well-posed.

$\pi_3[\mathcal{M}, L]$: \mathcal{M}, L -TUTTE POLYNOMIAL

Instance: matroid M belonging to a succinct class \mathcal{M} .

Output: $T(M; x(s), y(s))$ as a rational function of s in standard form.

Evidently $\pi_3[\mathcal{M}, L]$ is polynomial-time reducible to $\pi_1[\mathcal{M}]$ and, for any (a, b) in L , the problem $\pi_2[\mathcal{M}, a, b]$ is polynomial-time reducible to $\pi_3[\mathcal{M}, L]$.

The main theorems of [34] concern succinct expansion-closed classes of matroids where a class \mathcal{M} of matroids is *expansion-closed* if, for all M in \mathcal{M} and all positive integers k , the two matroids that are obtained from M by replacing each element by k elements in parallel and by replacing each element by k elements in series are both in \mathcal{M} ; and, from a succinct representation of M , one can construct succinct representations of these two expanded matroids in time that is polynomial in k and $|E(M)|$. Certain hyperbolae feature in the next two theorems, which are the main results of [34]. A curve $L = \{(x(s), y(s)) : s \in \mathbb{F}\}$ is *special* if $(x(s) - 1)(y(s) - 1)$ is constant. The first theorem asserts that determining the Tutte polynomial completely along a non-special curve is, to within a polynomial factor, no easier than determining it in the whole plane.

Theorem 8.1. *Let \mathcal{M} be a succinct expansion-closed class of matroids and L be a rational curve in \mathbb{F}^2 . Then the problem $\pi_1[\mathcal{M}]$ of determining the Tutte polynomial on the plane for members of \mathcal{M} is polynomial-time reducible to the problem $\pi_3[\mathcal{M}, L]$ of evaluating the Tutte polynomial for members of \mathcal{M} on the curve L , provided that L is not a special curve.*

The second theorem shows that, apart from nine special points, evaluating the Tutte polynomial at a point on a special curve is no easier than evaluating it along the whole special curve.

Theorem 8.2. *Let \mathcal{M} be a succinct expansion-closed class of matroids and L be a special curve in \mathbb{F}^2 . Then the problem $\pi_3[\mathcal{M}, L]$ of evaluating the Tutte polynomial for members of \mathcal{M} along L is polynomial-time reducible to the problem $\pi_2[\mathcal{M}, a, b]$ for any (a, b) on L provided (a, b) is not one of the nine points $(1, 1), (0, 0), (-1, -1), (0, -1), (-1, 0), (i, -i), (-i, i), (j, j^2)$, and (j^2, j) where $i^2 = -1$ and $j = e^{2\pi i/3}$.*

The next two results are consequences of the last two theorems. The first resolves the complexity status of the Jones polynomial. Before stating it, we describe the graph that one associates with an alternating link diagram D . The faces in such a link diagram can be coloured black and white so that adjacent faces receive different colours and the infinite face is coloured white. Let $S(D)$ be the simple graph whose vertices correspond to the black faces, with two such vertices being adjacent when the corresponding faces occur opposite each other at a crossing. If L is an alternating link and D a corresponding link diagram, Thistlethwaite [70] showed that, up to an easily derived factor, the Jones polynomial of L is given by an evaluation of the Tutte polynomial of $S(D)$ along the hyperbola $xy = 1$. The next corollary comes from combining this result with the last two theorems.

Corollary 8.3. *The problem of determining the Jones polynomial of an alternating link is $\#P$ -hard.*

When the last two theorems are specialized to graphs, one obtains the following result.

Corollary 8.4. *The problem of evaluating the Tutte polynomial of a graph at a point (a, b) is $\#P$ -hard except when (a, b) is on the hyperbola $(x - 1)(y - 1) = 1$ or when (a, b) is one of the special points $(1, 1), (-1, -1), (0, -1), (-1, 0), (i, -i), (-i, i), (j, j^2)$, and (j^2, j) where $i^2 = -1$ and $j = e^{2\pi i/3}$. In each of these exceptional cases, the evaluation can be done in polynomial time.*

The last theorem was extended for planar graphs by Dirk Vertigan [82] and then for bipartite planar graphs by Dirk and Dominic [83].

Theorem 8.5. *The problem of evaluating the Tutte polynomial of a bipartite planar graph at a point (a, b) is $\#P$ -hard except when (a, b) is on one of the hyperbolae $(x - 1)(y - 1) = 1$ and $(x - 1)(y - 1) = 2$, or when (a, b) is one of the special points $(1, 1), (-1, -1), (j, j^2)$, and (j^2, j) . In each of these exceptional cases, the evaluation can be done in polynomial time.*

A much more detailed discussion of the complexity issues considered above can be found in Dominic's book *Complexity: Knots, Colourings and Counting* and in Dominic's survey papers [105, 106]. Although it does not concern the Tutte polynomial specifically, it is appropriate to mention here a 1980 paper of Dominic with Gordon Robinson [63] on the complexity of matroid properties. That paper considers various different ways in which matroids could be presented via an oracle and then compares them.

9. CONCLUSION

Throughout his career, Dominic has actively promoted combinatorics in Britain. In addition to organizing numerous conferences, he served as Chair of the British Combinatorial Committee. In that role, he spoke at a reception dinner for participants at the 1985 British Combinatorial Conference hosted by the Lord Mayor of Glasgow. In his speech, Dominic indicated that, like so many other mathematicians, he worked in the subject because of its beauty. In G. H. Hardy's eloquent words on the links between mathematics and beauty, one thing stands out in relation to Dominic's work in matroid theory: "The best mathematics is serious as well as beautiful" [28, p. 29]. Dominic Welsh has had an enormous influence on the last forty years of the development of matroid theory. He has proved theorems showing that it is a serious area of study with important links to other more mainstream areas of mathematics. He has popularized the subject through his writing and his conjectures, and he has very generously and unselfishly shared both his time and his ideas with all in the pursuit of beautiful mathematics.

ACKNOWLEDGEMENTS

The author gratefully acknowledges the support provided by a Visiting Research Fellowship at Merton College for Trinity Term, 2005, and by a grant from the National Security Agency. Graham Farr and Michel Las Vergnas provided helpful comments on an earlier version of this paper.

REFERENCES

- [1] Martin Aigner, The Penrose polynomial of graphs and matroids, *Surveys in Combinatorics, 2001*, pp. 11–46, Cambridge University Press, Cambridge, 2001.
- [2] K. Appel and W. Haken, Every planar map is four-colorable, *Bull. Amer. Math. Soc.* **82** (1976), 711–712.
- [3] G. D. Birkhoff, A determinant formula for the number of ways of coloring a map, *Ann. Math. (2)*. **14** (1912–13), 42–46.
- [4] Béla Bollobás, A lower bound for the number of non-isomorphic matroids, *J. Combinatorial Theory* **7** (1969), 366–368.
- [5] J. A. Bondy, Transversal matroids, base-orderable matroids, and graphs, *Quart. J. Math. Oxford Ser. (2)* **23** (1972), 81–89.
- [6] J. A. Bondy and D. J. A. Welsh, Some results on transversal matroids and constructions for identically self-dual matroids, *Quart. J. Math. Oxford Ser. (2)* **22** (1971), 435–451.
- [7] Joseph Bonin, Anna de Mier, and Marc Noy, Lattice path matroids: enumerative aspects and Tutte polynomials, *J. Combin. Theory Ser. A* **104** (2003), 63–94.
- [8] O. Borůvka, O jistém problému minimálním, *Práce Mor. Přírodověd Spol. v. Brně (Acta Societ. Scient. Natur. Moraviae)* **3** (1926), 37–58.
- [9] R. L. Brooks, C. A. B. Smith, A. H. Stone, and W. T. Tutte, The dissection of rectangles into squares, *Duke Math. J.* **7** (1940), 312–340.
- [10] T. H. Brylawski, A decomposition for combinatorial geometries, *Trans. Amer. Math. Soc.* **171** (1972), 235–282.
- [11] Henry H. Crapo, Single-element extensions of matroids, *J. Res. Nat. Bur. Standards Sect. B* **69B** (1965), 55–65.

- [12] H. H. Crapo, The Tutte polynomial, *Aequationes Math.* **3** (1969), 211–229.
- [13] Henry Crapo and William Schmitt, The free product of matroids, *European J. Combin.* **26** (2005), 1060–1065.
- [14] H. H. Crapo and G.-C. Rota, *On the Foundations of Combinatorial Theory: Combinatorial Geometries*, Preliminary edition, MIT Press, Cambridge, 1970.
- [15] B. T. Datta, Nonexistence of six-dimensional tangential 2-blocks, *J. Combin. Theory Ser. B* **21** (1976), 1–22.
- [16] B. T. Datta, Nonexistence of seven-dimensional tangential 2-blocks, *Discrete Math.* **36** (1981), 1–32.
- [17] J. de Sousa and D. J. A. Welsh, A characterisation of binary transversal structures, *J. Math. Anal. Appl.* **40** (1972), 55–59.
- [18] G. A. Dirac, Some theorems on abstract graphs, *Proc. London Math. Soc. (3)* **2** (1952), 69–81.
- [19] T. A. Dowling, On the independent set numbers of a finite matroid, *Combinatorics 79. Part I* (eds. M. Deza and I. G. Rosenberg) Ann. Discrete Math. **8**, pp. 21–28, North-Holland, Amsterdam, 1980.
- [20] Jack Edmonds and D. R. Fulkerson, Transversals and matroid partition, *J. Res. Nat. Bur. Standards Sect. B* **69B** (1965), 147–153.
- [21] G. E. Farr, Tutte-Whitney polynomials: some history and generalisations, this volume.
- [22] Michael R. Garey and David S. Johnson, *Computers and Intractability. A Guide to the Theory of NP-Completeness*, W. H. Freeman and Co., San Francisco, 1979.
- [23] Geoffrey Grimmett and Dominic Welsh, *Probability: An Introduction*, Oxford University Press, New York, 1986.
- [24] H. Hadwiger, Über eine Klassifikation der Streckencomplexe, *Vierteljsch. Naturforsch. Ges. Zurich* **88** (1943), 133–142.
- [25] P. Hall, On representatives of subsets, *J. London Math. Soc.* **10** (1935), 26–30.
- [26] Y. O. Hamidoune and I. Salaiün, On the independence numbers of a matroid. *J. Combin. Theory Ser. B* **47** (1989), 146–152.
- [27] Frank Harary and Dominic Welsh, Matroids versus graphs, *The Many Facets of Graph Theory* (Proc. Conf., Western Mich. Univ., Kalamazoo, Mich., 1968), pp. 155–170, Springer, Berlin, 1969.
- [28] G. H. Hardy, *A Mathematician's Apology*, Cambridge University Press, Cambridge, 1948.
- [29] Winfried Hochstättler and Bill Jackson, Large circuits in binary matroids of large cogirth. I, II, *J. Combin. Theory Ser. B* **74** (1998), 35–52, 53–63.
- [30] Xiang-Dong Hou, On the asymptotic number of non-equivalent q -ary linear codes. *J. Combin. Theory Ser. A* **112** (2005), 337–346.
- [31] Xiang-Dong Hou, On the asymptotic number of non-equivalent binary linear codes, *Finite Fields Appl.* (2006), to appear.
- [32] F. Jaeger, On nowhere-zero flows in multigraphs, *Proc. British Combinatorial Conference* (eds. C. Nash-Williams and J. Sheehan), pp. 373–379, Congressus Numerantium **15**, Utilitas Mathematica, Winnipeg, 1976.
- [33] François Jaeger, Tutte polynomials and link polynomials, *Proc. Amer. Math. Soc.* **103** (1988), 647–654.
- [34] F. Jaeger, D. L. Vertigan, and D. J. A. Welsh, On the computational complexity of the Jones and Tutte polynomials, *Math. Proc. Camb. Phil. Soc.* **108** (1990), 35–53.
- [35] Vaughn F. R. Jones, A polynomial invariant for knots via von Neumann algebras, *Bull. Amer. Math. Soc.* **12** (1985), 103–111.
- [36] Donald E. Knuth, The asymptotic number of geometries, *J. Combin. Theory Ser. A* **17** (1974), 398–401.
- [37] Joseph P. S. Kung, *A Source Book in Matroid Theory*, Birkhäuser, Boston, 1986.

- [38] Joseph P. S. Kung, Excluding the cycle geometries of the Kuratowski graphs from binary geometries, *Proc. London Math. Soc. (3)* **55** (1987), 209–242.
- [39] Joseph P. S. Kung, Extremal matroid theory, *Graph Structure Theory* (Seattle, 1991), pp. 21–61, Contemp. Math., 147, Amer. Math. Soc., Providence, 1993.
- [40] Joseph P. S. Kung, Critical problems, *Matroid Theory* (Seattle, 1995), pp. 1–127, Contemp. Math., 197, Amer. Math. Soc., Providence, 1996
- [41] Michel Las Vergnas, Sur les systèmes de représentants distincts d’une famille d’ensembles, *C. R. Acad. Sci. Paris Sér. A-B* **270** (1970), A501–A503.
- [42] Michel Las Vergnas, Extensions normales d’un matroïde, polynôme de Tutte d’un morphisme, *C. R. Acad. Sci. Paris Sér. A-B* **280** (1975), A1479–A1492.
- [43] Michel Las Vergnas, The Tutte polynomial of a morphism of matroids. *Combinatorics 79* (Proc. Colloq., Univ. Montréal, 1979), Part I. *Ann. Discrete Math.* **8** (1980), 7–20.
- [44] Michel Las Vergnas, The Tutte polynomial of a morphism of matroids. I. Set-pointed matroids and matroid perspectives (Symposium à la Mémoire de François Jaeger, Grenoble, 1998), *Ann. Inst. Fourier (Grenoble)* **49** (1999), 973–1015.
- [45] Michel Las Vergnas, The Tutte polynomial of a morphism of matroids. 5. Computational complexity, *Portugal. Math* (2006), to appear.
- [46] R. F. Lax, On the character of S_n acting on subspaces of \mathbb{F}_q^n , *Finite Fields Appl.* **10** (2004), 315–322.
- [47] Manoel Lemos, On the number of non-isomorphic matroids, *Adv. in Appl. Math.* **33** (2004), 733–746.
- [48] Bernt Lindström, On the chromatic number of regular matroids, *J. Combin. Theory Ser. B* **24** (1978), 367–369.
- [49] Carolyn Mahoney, On the unimodality of the independent set numbers of a class of matroids, *J. Combin. Theory Ser. B* **39** (1985), 77–85.
- [50] J. H. Mason, Matroids: unimodal conjectures and Motzkin’s theorem, *Combinatorics* (eds. D. J. A. Welsh and D. R. Woodall), pp. 207–220, Institute of Math. and its Applications, Southend-on-Sea, 1972.
- [51] L. Mirsky, *Transversal Theory*, Academic Press, New York, London, 1971.
- [52] L. Mirsky and Hazel Perfect, Systems of representatives, *J. Math. Anal. Appl.* **15** (1966), 520–568.
- [53] L. Mirsky and Hazel Perfect, Applications of the notion of independence to problems of combinatorial analysis, *J. Combinatorial Theory* **2** (1967), 327–357.
- [54] Oystein Ore, Graphs and matching theorems, *Duke Math. J.* **22** (1955), 625–639.
- [55] James G. Oxley, *Matroid Theory*, Oxford University Press, New York, 1992.
- [56] J. G. Oxley and D. J. A. Welsh, The Tutte polynomial and percolation, *Graph Theory and Related Topics* (eds. J. A. Bondy and U. S. R. Murty), pp. 329–339, Academic Press, London, 1979.
- [57] James Oxley and Geoff Whittle, A characterization of Tutte invariants of 2-polymatroids, *J. Combin. Theory Ser. B* **59** (1993), 210–244.
- [58] M. J. Piff, An upper bound for the number of matroids, *J. Combinatorial Theory Ser. B* **14** (1973), 241–245.
- [59] M. J. Piff and D. J. A. Welsh, On the vector representation of matroids. *J. London Math. Soc. (2)* **2** (1970), 284–288.
- [60] M. J. Piff and D. J. A. Welsh, The number of combinatorial geometries, *Bull. London Math. Soc.* **3** (1971), 55–56.
- [61] R. Rado, A theorem on independence relations, *Quart. J. Math., Oxford Ser.* **13** (1942), 83–89.
- [62] R. Rado, On the number of systems of distinct representatives of sets, *J. London Math. Soc.* **42** (1967), 107–109.
- [63] G. C. Robinson and D. J. A. Welsh, The computational complexity of matroid properties, *Math. Proc. Cambridge Philos. Soc.* **87** (1980), 29–45.

- [64] G.-C. Rota, On the foundations of combinatorial theory I, *Z. Wahrsch.* **2** (1964), 340–368.
- [65] P. D. Seymour, *Matroids, Hypergraphs and the Max-Flow Min-Cut Theorem*, D.Phil. thesis, University of Oxford, 1975.
- [66] P. D. Seymour, Decomposition of regular matroids, *J. Combin. Theory Ser. B* **28** (1980), 305–359.
- [67] P. D. Seymour, Nowhere-zero 6-flows, *J. Combin. Theory Ser. B* **30** (1981), 130–135.
- [68] P. D. Seymour, On Tutte’s extension of the four-colour problem, *J. Combin. Theory Ser. B* **31** (1981), 82–94.
- [69] John Talbot and Dominic Welsh, *Cryptography and Complexity*, Cambridge University Press, Cambridge, 2005.
- [70] M. B. Thistlethwaite, A spanning tree expansion of the Jones polynomial, *Topology* **26** (1987), 297–309.
- [71] R. Thomas, Recent excluded minor theorems for graphs, *Surveys in Combinatorics, 1999* (eds. J. D. Lamb and D. A. Preece), pp. 201–222, Cambridge University Press, Cambridge, 1999.
- [72] W. T. Tutte, A ring in graph theory, *Proc. Camb. Phil. Soc.* **43** (1947), 26–40.
- [73] W. T. Tutte, *An Algebraic Theory of Graphs*, Ph.D. thesis, Cambridge University, 1948.
- [74] W. T. Tutte, A contribution to the theory of chromatic polynomials, *Canad. J. Math.* **6** (1954), 80–91.
- [75] W. T. Tutte, A homotopy theorem for matroids. I, II, *Trans. Amer. Math. Soc.* **88** (1958), 144–160, 161–174.
- [76] W. T. Tutte, Matroids and graphs, *Trans. Amer. Math. Soc.* **90** (1959), 527–552.
- [77] W. T. Tutte, On the algebraic theory of graph colorings, *J. Combin. Theory Ser. B* **1** (1966), 15–50.
- [78] W. T. Tutte, On dichromatic polynomials, *J. Combin. Theory* **2** (1967), 301–320.
- [79] W. T. Tutte, A geometrical version of the four color problem, *Combinatorial Mathematics and its Applications* (eds. R. C. Bose and T. A. Dowling), pp. 553–561, University of North Carolina Press, Chapel Hill, 1969.
- [80] W. T. Tutte, *Introduction to the Theory of Matroids*, American Elsevier, New York, 1971.
- [81] W. T. Tutte, *Graph Theory as I Have Known It*, Oxford University Press, Oxford, 1998.
- [82] Dirk Vertigan, *On the Computational Complexity of Tutte, Jones, Homfly and Kauffman Invariants*, D. Phil. thesis, University of Oxford, 1991.
- [83] D. L. Vertigan and D. J. A. Welsh, The computational complexity of the Tutte plane: the bipartite case, *Combin. Probab. Comput.* **1** (1992), 181–187.
- [84] P. N. Walton and D. J. A. Welsh, On the chromatic number of binary matroids, *Mathematika* **27** (1980), 1–9.
- [85] P. N. Walton and D. J. A. Welsh, Tangential 1-blocks over $\text{GF}(3)$, *Discrete Math.* **40** (1982), 319–320.
- [86] K. Wagner, Über eine Eigenschaft der ebenen Komplexe, *Math. Ann.* **114** (1937), 570–590.
- [87] D. J. A. Welsh, Kruskal’s theorem for matroids, *Proc. Cambridge Philos. Soc.* **64** (1968), 3–4.
- [88] D. J. A. Welsh, Some applications of a theorem of Rado, *Mathematika* **15** (1968), 199–203.
- [89] D. J. A. Welsh, Euler and bipartite matroids, *J. Combinatorial Theory* **6** (1969), 375–377.
- [90] D. J. A. Welsh, A bound for the number of matroids, *J. Combinatorial Theory* **6** (1969), 313–316.

- [91] D. J. A. Welsh, Transversal theory and matroids, *Canad. J. Math.* **21** (1969), 1323–1330.
- [92] D. J. A. Welsh, On matroid theorems of Edmonds and Rado. *J. London Math. Soc.* (2) **2** (1970), 251–256.
- [93] D. J. A. Welsh (editor), *Combinatorial Mathematics and its Applications* (Proc. Conf., Oxford, 1969), Academic Press, London, 1971.
- [94] D. J. A. Welsh, Combinatorial problems in matroid theory, *Combinatorial Mathematics and its Applications* (Proc. Conf., Oxford, 1969), pp. 291–306, Academic Press, London, 1971.
- [95] D. J. A. Welsh, Generalized versions of Hall’s theorem, *J. Combinatorial Theory Ser. B* **10** (1971), 95–101.
- [96] D. J. A. Welsh, *Matroid Theory*, Academic Press, London, New York, 1976.
- [97] D. J. A. Welsh, Colouring problems and matroids, *Surveys in Combinatorics* (ed. B. Bollobás), pp. 229–257, Cambridge University Press, Cambridge, 1979.
- [98] D. J. A. Welsh, Colourings, flows and projective geometry, *Nieuw Arch. Wisk.* (3) **28** (1980), 159–176.
- [99] D. J. A. Welsh, Matroids and combinatorial optimisation, *Matroid Theory and its Applications*, pp. 323–416, Liguori, Naples, 1982.
- [100] Dominic Welsh, *Codes and Cryptography*, Oxford University Press, New York, 1988.
- [101] Dominic Welsh, Matroids and their applications, *Selected Topics in Graph Theory, 3* (eds. R. J. Wilson and L. W. Beineke), pp. 43–70, Academic Press, San Diego, 1988.
- [102] D. J. A. Welsh, *Complexity: Knots, Colourings and Counting*, London Mathematical Society Lecture Note Series, 186, Cambridge University Press, Cambridge, 1993.
- [103] D. J. A. Welsh, The computational complexity of knot and matroid polynomials, *Discrete Math.* **124** (1994), 251–269.
- [104] D. J. A. Welsh, Matroids: fundamental concepts, *Handbook of Combinatorics, Vol. 1, 2*, pp. 481–526, Elsevier, Amsterdam, 1995.
- [105] Dominic Welsh, Approximate counting, *Surveys in Combinatorics, 1997*, pp. 287–323, Cambridge University Press, Cambridge, 1997.
- [106] Dominic Welsh, The Tutte polynomial, *Random Structures Algorithms* **15** (1999), 210–228.
- [107] D. J. A. Welsh and K. K. Kayibi, A linking polynomial of two matroids, *Adv. in Appl. Math.* **32** (2004), 391–419.
- [108] Dominic J. A. Welsh and Geoffrey P. Whittle, Arrangements, channel assignments, and associated polynomials, *Adv. in Appl. Math.* **23** (1999), 375–406.
- [109] D. J. A. Welsh and D. R. Woodall, *Combinatorics* (Proc. Conf. on Combinatorial Math., Oxford, 1972), The Institute of Mathematics and its Applications, Southend-on-Sea, 1972.
- [110] N. White (editor), *Theory of Matroids*, Cambridge University Press, Cambridge, 1986.
- [111] N. White (editor), *Combinatorial Geometries*, Cambridge University Press, Cambridge, 1987.
- [112] N. White (editor), *Matroid Applications*, Cambridge University Press, Cambridge, 1992.
- [113] H. Whitney, The coloring of graphs, *Ann. Math.* (2) **33** (1932), 688–718.
- [114] H. Whitney, On the abstract properties of linear dependence, *Amer. J. Math.* **57** (1935), 509–533.
- [115] Geoff Whittle, Modularity in tangential k -blocks, *J. Combin. Theory Ser. B* **42** (1987), 24–35.
- [116] Geoffrey Whittle, Quotients of tangential k -blocks, *Proc. Amer. Math. Soc.* **102** (1988), 1088–1098.
- [117] Geoff Whittle, q -lifts of tangential k -blocks, *J. London Math. Soc.* (2) **39** (1989), 9–15.

- [118] Geoff Whittle, Dowling group geometries and the critical problem. *J. Combin. Theory Ser. B* **47** (1989), 80–92.
- [119] Marcel Wild, The asymptotic number of inequivalent binary codes and nonisomorphic binary matroids, *Finite Fields Appl.* **6** (2000), 192–202.
- [120] Marcel Wild, The asymptotic number of binary codes and binary matroids, *SIAM J. Discrete Math.* **19** (2005), 691–699.

DEPARTMENT OF MATHEMATICS, LOUISIANA STATE UNIVERSITY, BATON ROUGE,
LOUISIANA, USA

E-mail address: `oxley@math.lsu.edu`