Math. Proc. Camb. Phil. Soc. (1990), **108**, 35
Printed in Great Britain

On the computational complexity of the Jones and Tutte polynomials

BY F. JAEGER
Laboratoire de Structures Discrètes, Institut IMAG, Grenoble, France

D. L. VERTIGAN AND D. J. A. WELSH
Merton College and the Mathematical Institute, University of Oxford

(*Received* 26 *June* 1989; *revised* 6 *December* 1989)

Abstract

We show that determining the Jones polynomial of an alternating link is $\#P$-hard. This is a special case of a wide range of results on the general intractibility of the evaluation of the Tutte polynomial $T(M;x,y)$ of a matroid M except for a few listed special points and curves of the (x,y)-plane. In particular the problem of evaluating the Tutte polynomial of a graph at a point in the (x,y)-plane is $\#P$-hard except when $(x-1)(y-1)=1$ or when (x,y) equals $(1,1)$, $(-1,-1)$, $(0,-1)$, $(-1,0)$, $(i,-i)$, $(-i,i)$, (j,j^2), (j^2,j) where $j=e^{2\pi i/3}$.

1. *Introduction*

The original problem motivating this paper is to decide whether or not computing the Jones polynomial of a link is, in general, a feasible computation. To put this question in perspective, it is well known that computation of the Alexander–Conway polynomial of a link is 'easy' (that is, can be done in time polynomial in the size of the input) being just the expansion of a one-variable determinant, but that the computations of the Homfly and Kauffman polynomials of a link are NP-hard (Jaeger[**15**], Thistlethwaite[**40**]). The Jones polynomial could be regarded as lying somewhere between the Alexander–Conway polynomial and these two other link polynomials in terms of computational difficulty. However, as we shall see, it turns out to be computationally intractable in a very strong sense, even for the special case of alternating links.

To obtain this result we use intimate relationships between links, graphs and matroids representable over various fields. The common basic concept is the Tutte polynomial $T(M;x,y)$ (or equivalently the Whitney rank generating function) of a matroid M. For cycle matroids of planar graphs, this two-variable polynomial specializes along a particular hyperbola of the plane to the Jones polynomial of an alternating link (up to a normalization factor). Many other specializations of the Tutte polynomial are known, in areas as diverse as statistical mechanics (via the Ising and Potts models), percolation and reliability theory, colouring and flows in graphs and in determining the weight enumerator of a code. Details of some of these specializations are given in Section 2.

As far as the notions of computational complexity are concerned, one of its main aims is to classify and explain the gulf that separates tractable problems from the apparently intractable. We will now briefly review the main ideas of complexity as applied to enumerative problems.

We will regard a computational problem as a function mapping instances to solutions (a link diagram to its Jones polynomial, for example). A problem is *polynomial time computable* if there exists an algorithm which computes this function in a length of time (number of steps) bounded by a polynomial in the size of the problem instance. The class of such problems we denote by P. As usual the formal model of computation is the Turing machine and if A, B are two problems we say that A is *polynomial time (Turing) reducible* to B, written $A \propto B$, if it is possible with the aid of an oracle (or sub-routine) for problem B to solve A in polynomial time (in other words, counting calls to the B-oracle as a single step the number of steps needed to solve A is polynomially bounded).

The class $\#P$ can be described informally as the class of enumeration problems in which the structures being counted are recognizable in polynomial time, that is, there is an algorithm which 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.

For example, suppose the problem is to count the number of truth assignments of a Boolean formula of length n in conjunctive normal form. Since it is easy to check in time polynomial in n whether a given assignment satisfies the given formula, the problem of counting the satisfying assignments is in the class $\#P$. Thus the class $\#P$ is the enumerative analogue of the more well known class NP of decision problems solved in polynomial time by a non-deterministic Turing machine.

What makes $\#P$ important is that it contains problems called $\#P$-complete problems which are proven to be at least as hard as any problem in the class. A problem A in $\#P$ is *$\#P$-complete* if for any problem B in $\#P$, B is polynomial-time reducible to A. If a polynomial time algorithm were found for any such problem it would follow that $\#P \subseteq P$.

Examples of $\#P$-complete problems are the counting of truth assignments for a Boolean formula in conjunctive normal form, counting the number of Hamiltonian paths in a graph, evaluating the permanent of a square $(0, 1)$ matrix, together with several of the more intractable enumerative problems of statistical physics.

In the same way as a problem is described as *NP-hard* if some NP-complete problem is polynomial time reducible to it, a problem is *$\#P$-hard* if some $\#P$-complete problem is polynomial time reducible to it. If a problem π is $\#P$-hard, then the existence of a polynomial time algorithm for π would imply the existence of such an algorithm for all problems in $\#P$. Since $\#P$ contains such notoriously intractable problems as those mentioned above, proving that a problem is $\#P$-hard is very strong evidence of its computational intractability.

For a precise and more formal treatment of these ideas see Garey and Johnson [**10**] or Valiant [**43**].

We shall show in Section 6 that determining the Jones polynomial of an alternating link is $\#P$-hard. To do this we use its relationship with the Tutte polynomial of an associated planar graph [**39**]. In fact we obtain more general results on the computational complexity of other well known polynomials associated with graphs, codes and matroids.

The reader will notice that many of our results will show that certain evaluations and computations are *#P-hard*. We should draw attention to the point that in every case they are also polynomial time Turing reducible to any #*P*-complete problem. However, in general, they are not #*P*-complete themselves because they are not, strictly speaking, members of #*P*.

2. *Matroids and the Tutte polynomial*

The Tutte polynomial was originally defined by W. T. Tutte for graphs [**41**] and is closely related to an earlier graph polynomial introduced by Whitney [**47**]. Both polynomials have a natural extension to matroids [**4**, **8**] in which context they have several different interesting interpretations. The graph terminology we use is standard; see for instance [**3**]. A *matroid* can be defined in many equivalent ways (see [**45**]) but it is probably simplest here to regard it as a pair $M = (S, \rho)$ where S is a finite *ground set* and $\rho : 2^S \to \mathbb{Z}$ is the *rank function* and satisfies the conditions (i) $0 \leqslant \rho(A) \leqslant |A|$ for all $A \subseteq S$, (ii) $\rho(X) \leqslant \rho(Y)$ for $X \subseteq Y \subseteq S$, (iii) ρ is *submodular*, that is for any two subsets X, Y of S,

$$\rho(X \cup Y) + \rho(X \cap Y) \leqslant \rho(X) + \rho(Y).$$

A subset of S is *independent* in M if its rank equals its cardinality, it is a *base* if it is a maximal independent set and it is *spanning* if its rank equals the rank of S. It is now easy to recognize a matroid as an abstraction of the idea of linear independence as originally proposed by Whitney [**48**]. It can be shown that the collection of its independent sets or spanning sets or bases uniquely determines a matroid.

Associated with every matroid $M = (S, \rho)$ is its *dual matroid* $M^* = (S, \rho^*)$ with rank function defined by

$$\rho^*(A) = |A| + \rho(S - A) - \rho(S) \quad \text{for every} \quad A \subseteq S.$$

Note that $(M^*)^* = M$ and the independent sets, spanning sets, bases of M^* are the complements respectively of the spanning sets, independent sets, bases of M.

An element e of S is a *loop* of M if $\rho(\{e\}) = 0$, and is a *coloop* of M if it is a loop of M^*.

Two matroids are *isomorphic* if there is a bijection between their ground sets which preserves rank function (and hence independent sets, etc.) in the obvious way.

The matroid $M = (S, \rho)$ is *coordinatizable* or *representable* over a particular field if there exists a vector space V over that field and a map $\phi : S \to V$ such that A is independent in M if and only if $\phi(A)$ is a collection of linearly independent vectors of V. A matroid is *binary* (*ternary*) if it is representable over $\mathbb{F}_2$ (respectively $\mathbb{F}_3$).

For any graph $G = (V, E)$ we denote by $M(G)$ the *cycle matroid* on the ground set E whose independent sets are those collections of edges which contain no cycle. A matroid is *graphic* if it is isomorphic to the cycle matroid of some graph. It is easily shown that every graphic matroid is coordinatizable over every field. When M is the cycle matroid of a plane graph its dual matroid is the cycle matroid of the dual plane graph. For further details of the relationship between graphs, matroids and representability we refer to the original paper of Whitney [**48**] or the monograph of Welsh [**45**].

Two fundamental constructions in matroid theory, and particularly in the theory of the Tutte polynomial are the following Let $M = (S, \rho)$ and $e \in S$. The *deletion* of e from M is the matroid $M\backslash e = (S\backslash\{e\}, \rho')$ where $\rho'(A) = \rho(A)$ for every $A \subseteq S\backslash\{e\}$. The *contraction* of e from M is the matroid $M/e = (S\backslash\{e\}, \rho'')$ where $\rho''(A) = \rho(A \cup \{e\}) - \rho(\{e\})$ for every $A \subseteq S\backslash\{e\}$, or equivalently $M/e = (M^*\backslash e)^*$. In particular for a graph G, deletion and contraction in $M(G)$ correspond to deletion and contraction of edges in the graph. Any matroid obtained from M by a sequence of deletions and contractions is a *minor* of M. It can be shown that the order in which the deletions and contractions are done does not affect the result.

A less familiar notion is the following. Let $M = (S, \rho)$ and $N = (T, \lambda)$ be two matroids on disjoint ground sets S and T, and let $e \in S$, $f \in T$. For $A \subseteq S\backslash\{e\}$ and $B \subseteq T\backslash\{f\}$, define $\delta(A, B)$ to be 1 if $\rho(A) = \rho(A \cup \{e\})$ and $\lambda(B) = \lambda(B \cup \{f\})$, and to be 0 otherwise. The 2-*sum* of M and N at elements e and f is the matroid on ground set $(S \cup T)\backslash\{e, f\}$ for which the rank of $A \cup B$ is

$$\rho(A) + \lambda(B) - \delta(A, B) + \delta(\varnothing, \varnothing).$$

For instance, if $M = M(G)$ and $N = M(H)$ for two disjoint graphs G, H, the 2-sum of M and N corresponds to the identification of the edges e and f into a new edge which is then deleted. The concept of 2-sum was introduced by Seymour [**36**] and is closely related to the parallel connection introduced earlier by Brylawski [**4**]. It is of crucial importance in our proofs, in particular in the use of Brylawski's *tensor product* [**6**] of matroids which we introduce in Section 7.

Let $M = (S, \rho)$ be a matroid. Its *Whitney rank generating function* $R(M; x, y)$ is defined by

(2·1) $$R(M; x, y) = \sum_{A \subseteq S} x^{\rho(S) - \rho(A)} y^{|A| - \rho(A)}.$$

Its *Tutte polynomial* $T(M; x, y)$ is defined by

(2·2) $$T(M; x, y) = R(M; x-1, y-1).$$

Basic properties of the Tutte polynomial are given below.

(2·3) If M^* denotes the dual of M then $T(M^*; x, y) = T(M; y, x)$.

(2·4) $T(M; 1, 1)$ counts the number of bases of M.

(2·5) $T(M; 2, 1)$ counts the number of independent sets of M.

(2·6) $T(M; 1, 2)$ counts the number of spanning sets of M.

(2·7) When $M = M(G)$ and G is a graph with vertex set $\{v_1, \ldots, v_n\}$, the *score vector* associated with an orientation of G is the ordered n-tuple $(s_1, \ldots, s_n)$ where s_i is the number of edges oriented away from v_i. It is shown in [**38**] that $T(M; 2, 1)$ is the number of distinct score vectors of G.

(2·8) When M is graphic Rosenstiehl and Read [**35**] show that

$$T(M; -1, -1) = (-1)^{|E|}(-2)^{d(B)},$$

where B is the binary bicycle space of M and d denotes dimension. This is easily extended to binary matroids.

(2·9) When M is a ternary matroid, then for $j = e^{2i\pi/3}$,

$$|T(M; j, j^2)| = (\sqrt{3})^{d(B)},$$

where B is the ternary bicycle space of any ternary representation of M and d denotes dimension (see Jaeger [**16**]).

(2·10) When $M = M(G)$ for some graph G, $T(M;2,0)$ counts the number of acyclic orientations of G (see Stanley [**38**]). This has been generalized to regular matroids [**5**], matroids representable over $\mathbb{R}$ [**49**] and oriented matroids [**24**].

(2·11) When $M = M(G)$, and m is a positive integer, if $W(G,m)$ denotes the number of pairs (θ,ϕ) such that θ is an acyclic orientation of G and $\phi: V(G) \to \{1,2,\ldots,m\}$ is such that $\phi(u) \geqslant \phi(v)$ for every edge of G directed from u to v, then from [**38**], $T(M(G);m+1,0) = W(G;m)$. When $m = 1$ this reduces to (2·10).

(2·12) If G is a graph with k connected components and $M = M(G)$ then

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

where $P(G;\lambda)$ is the chromatic polynomial of G, which when λ is a positive integer n counts the number of vertex colourings of G using n colours.

(2·13) If $G = (V,E)$ is a graph and $M = M(G)$, and H is any abelian group of finite order h, the number of *nowhere zero flows* with values in H (see [**17**]) on the edges of G (with respect to an arbitrary orientation) is denoted by $F(G;H)$ and is given by

$$F(G;H) = (-1)^{|E|-\rho(M)} T(M;0,1-h).$$

This evaluation gives one of the most interesting Tutte–Grothendieck invariants, and at the same time one of the quickest proofs of the curious fact that the number of such flows only depends on the order of the group H.

Suppose now that for $a \in \mathbb{C}$ we let

(2·14) $H_a = \{(x,y): (x-1)(y-1) = a\}$.

Then it is trivial to use (2·1) and (2·2) to verify

(2·15) for any matroid M and point $(x,y) \in H_1$

$$T(M;x,y) = x^n (x-1)^{r-n},$$

where n is the size and r the rank of M.

(2·16) When M is the cycle matroid of a graph G and $(x,y) \in H_2$, the Tutte polynomial of M evaluates the partition function of the Ising model on G (see [**1**]).

(2·17) If $\mathscr{C}$ is a linear code of length n and dimension r over the finite field $\mathbb{F}_q$ the weight enumerator $A_q(\mathscr{C},z)$ of $\mathscr{C}$ (see [**29**]) is given by

$$A_q(\mathscr{C},z) = (1-z)^r z^{n-r} T\left(M; \frac{1+(q-1)z}{1-z}, \frac{1}{z}\right),$$

where M is the matroid induced on the set of columns of a generator matrix of $\mathscr{C}$ with independence defined by linear independence over $\mathbb{F}_q$ (see [**12**]).

In other words, using a suitable parametrization, along the hyperbola H_q, T evaluates the weight enumerator of $\mathscr{C}$.

Apart from the axes and the integer hyperbolae, another 'curve' on which T has an interesting interpretation is the line $x = 1$.

(2·18) For any connected graph $G = (V,E)$ and real q with $0 < q < 1$, suppose that each edge of G is, independently of all other edges, removed with probability q or retained with probability $p = 1-q$. We denote by $Q(G;p)$ the *percolation probability* which is the probability that the resulting random subgraph of G connects all the vertices of G. Then as noted in [**31**], we have

$$Q(G;p) = q^{|E|-\rho(G)} p^{\rho(G)} T(M(G);1,1/q).$$

(2·19) Along the hyperbola H_q, the Tutte polynomial of $M(G)$ gives the q-state Potts model of statistical mechanics (see Baxter[**1**]). This generalizes (2·16) which corresponds to the case $q = 2$.

(2·20) A much more important evaluation as regards this paper is along the hyperbola $xy = 1$, on which curve T specializes to the Jones polynomial of a link. See Thistlethwaite[**39**]. We return to this specialization in Section 6.

3. *The complexity of the Tutte polynomial*

The fundamental algorithmic problem with which we are concerned is the following.

(P1) For a given class $\mathscr{C}$ of matroids is there an algorithm which will compute the Tutte polynomial of any member of the class $\mathscr{C}$ in time polynomial in the size of the matroid?

Here we call the *size* of a matroid the cardinality of its ground set.

Note that $T(M; x, y)$ has a description of length polynomial in the size n of M as a list of n^2 integer coefficients each of length $O(n)$.

Ideally we would like to be able to carry out the computation in time which is a polynomial function of n, the size of the matroid. However, for the class of all matroids, this is not possible. If $f(n)$ denotes the number of non-isomorphic matroids on a set of n elements then it is known [**45**] that

$$2^{2^{n-\frac{3}{2}\log n+O(\log\log n)}} \leqslant f(n) \leqslant 2^{2^{n-\frac{1}{2}\log n+O(\log\log n)}}.$$

Hence there are too many matroids of size n for it to be possible even to describe (or input) the matroid to the algorithm (machine) in time which is subexponential in n. In other words for the class of *all* matroids the natural size of the input is $O(2^n)$. On the other hand there is a standard algorithm for determining the Tutte polynomial of a matroid using a recursive formula which expresses $T(M)$ in terms of $T(M\backslash e)$ and $T(M/e)$ for any element e. This takes time which is exponential in n.

A study of the computational complexity of general matroid properties has been carried out by Robinson and Welsh[**34**]. However, here we are concerned with practical questions concerning relatively special classes such as graphic and binary matroids.

If $\mathscr{C}$ is the class of graphic (binary) matroids on n elements then it is clearly possible to specify completely the matroid in a length which is polynomial in n (a graph with n edges or an r by n matrix of zeros and ones).

Hence in order that our original question (P1) about polynomial time complexity should make sense we impose the following restriction in terms of the representation or description of the matroids in a class.

We say that a class $\mathscr{C}$ of matroids has a *succinct description* or is *succinct* if there is an injective mapping (or encoding) e of the members of $\mathscr{C}$ into strings from some finite alphabet Σ, such that if $|e(M)|$ denotes the length (number of symbols) of $e(M)$,

$$\mathscr{C}_n = \{M \in \mathscr{C}, M = (S, \rho), |S| = n\} \quad \text{and} \quad e(n) = \max\{|e(M)| : M \in \mathscr{C}_n\}$$

then there exists some polynomial p such that $e(n) \leqslant p(n)$ for all n. It is clear that a class $\mathscr{C}$ has a succinct description if and only if $|\mathscr{C}_n|$ is $O(2^{q(n)})$ for some polynomial q. But in fact we shall be interested only in 'concrete' succinct descriptions which

satisfy certain compatibility requirements (see Section 4), although we do not feel it necessary to formalize this concept.

Although this seems excessively formal, it is usually easy to see that such an encoding e exists, as the following examples show.

Example (*a*). When $\mathscr{C}$ is the class of graphic matroids there is a natural encoding of $M \in \mathscr{C}$ by the vertex edge incidence matrix of any graph G such that $M = M(G)$.

Example (*b*). When $\mathscr{C}$ is the class of binary matroids and $M \in \mathscr{C}$ has rank r and size n we can represent M by any $r \times n$-matrix A of zeros and ones such that M is isomorphic to the matroid induced on the columns of A by linear independence over the field $\mathbb{F}_2$. A similar presentation is assumed when we are dealing with matroids represented over any finite field.

These two examples show that the classes of graphic and binary matroids are succinct, as are many other classes which arise naturally in examples.

In what follows we shall only be concerned with succinct classes and moreover it is important because of complexity considerations that when we speak of matroids belonging to any of these classes we *assume* that they are being described in some standard succinct description, for example graphs by incidence matrices, binary matroids by some minimal binary matrix representation and so on.

The problem (P1) which we described loosely earlier can now be more precisely posed in what has become the standard format of complexity theory (see [**10**]).

$\pi_1[\mathscr{C}]$: $\mathscr{C}$-TUTTE POLYNOMIAL

Instance: matroid M belonging to the succinct class $\mathscr{C}$.

Output: the Tutte polynomial of M.

For all but the most trivial classes $\mathscr{C}$ this problem will be $\#P$-hard. For example when $\mathscr{C}$ is the class of cycle matroids of planar graphs the above problem contains that of counting the 3-colourings of the vertices of a planar graph which is known to be $\#P$-complete. An explicit reference for this result (which is part of the 'folklore' of the complexity of enumeration problems) is hard to locate. It would be natural to expect that the transformation used by Garey, Johnson and Stockmeyer [**11**] in their proof that the corresponding decision problem (3-colouring planar graphs) is *NP*-complete is what is called a parsimonious transformation. This turns out to be not the case. However, a modification of their transformation communicated to us by M. Jerrum [**20**] does give a parsimonious transformation and thus gives an explicit 'constructive' proof. An alternative proof is to use the padding technique introduced by Berman and Hartmanis [**2**] in their proofs that the enumeration problems associated with the well known *NP*-complete problems are $\#P$-complete.

As seen in Section 2 it is also of interest to determine the Tutte polynomial $T(x, y)$ at particular points and along particular curves in the (x, y)-plane. When examining the complexity of these computations, it is necessary to consider how numbers are encoded as finite strings from some finite alphabet, and how arithmetic operations are performed on these. This problem is considered in more detail in [**13**] and [**43**]. If we want to work within a field F, say, then clearly F must be countable. Also there must be polynomial time algorithms for the various arithmetical operations to be used. In any polynomial time algorithm or Turing reduction using these operations, it is necessary that both the number of arithmetic operations

performed, and the length of the results, are polynomially bounded. This depends on the field and the encoding of its elements. For our purposes we choose the field F to be a finite-dimensional algebraic extension of the rationals. Elements of F can be represented as vectors with rational entries, and arithmetic reduced to rational arithmetic which has been well studied in the complexity of enumeration problems: see [43]. For reasons to become apparent in Section 4, F should contain the complex numbers i and $j = e^{2\pi i/3}$.

The problem of evaluating T at a point (a, b), where $a, b \in F$ can now be formulated precisely as follows:

(π_2): $\mathscr{C}$-TUTTE POLYNOMIAL EVALUATION at (a, b)
Instance: matroid M belonging to the succinct class $\mathscr{C}$.
Output: $T(M; a, b)$.

Abbreviating this problem to $\pi_2[\mathscr{C}, a, b]$, it is obvious that for any $\mathscr{C}, a, b$, we have

$$\pi_2[\mathscr{C}, a, b] \propto \pi_1[\mathscr{C}]. \tag{3·1}$$

Finally consider the problem of evaluating T along a curve L in the (x, y)-plane. We restrict our attention to the case where L is a rational curve, that is the set of points parameterized in standard form by

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

where u, v, w, z are given polynomials in $F[s]$. By a rational function in *standard form* we mean that the numerator and denominator are relatively prime and the denominator has leading coefficient one. A rational function can easily be put in standard form in polynomial time using Euclid's algorithm. Then along L the Tutte polynomial of M will be a rational function of s and hence the following is a well posed computational problem.

(π_3): $\mathscr{C}, L$-TUTTE POLYNOMIAL
Instance: matroid M belonging to the succinct class $\mathscr{C}$.
Output: $T(M; x(s), y(s))$ as a rational function of s in standard form.

We denote this problem by $\pi_3[\mathscr{C}, L]$ and make the obvious remarks

$$\pi_3[\mathscr{C}, L] \propto \pi_1[\mathscr{C}], \tag{3·2}$$

and for any $(a, b) \in L$

$$\pi_2[\mathscr{C}, a, b] \propto \pi_3[\mathscr{C}, L]. \tag{3·3}$$

Our results in Section 4 show that in many cases the converse polynomial time reduction holds for (3·2) or (3·3).

4. *Statement of the main theorems*

In order to present and prove our results we need some further definitions.

A *pointed* matroid N_d is a matroid on a ground set which includes a distinguished element, the point d, which will be assumed to be neither a loop or coloop. For ease

of notation we will let N denote N_d and then define the *tensor product* $M \otimes N$ of an arbitrary matroid M with the pointed matroid N as the matroid obtained by taking a 2-sum of M with N at *each* point e of M and the distinguished point d of N. For further details see Brylawski [6] or Brylawski and Oxley [7].

The Tutte polynomial of $M \otimes N$, where $M = (S, \rho)$ is then given by

$$T(M \otimes N; x, y) = T_C(N; x, y)^{|S|-\rho(S)} T_L(N; x, y)^{\rho(S)} T(M; X, Y) \tag{4·1}$$

where

$$X = \frac{(x-1)\, T_C(N; x, y) + T_L(N; x, y)}{T_L(N; x, y)}, \quad Y = \frac{T_C(N; x, y) + (y-1)\, T_L(N; x, y)}{T_C(N; x, y)}$$

and where T_C, T_L are polynomials which are determined by the equations

$$\left.\begin{aligned} (x-1)\, T_C(N; x, y) + T_L(N; x, y) &= T(N \backslash d; x, y), \\ T_C(N; x, y) + (y-1)\, T_L(N; x, y) &= T(N/d; x, y). \end{aligned}\right\} \tag{4·2}$$

We observe that taking the tensor product with a pointed matroid N gives rise to a transformation $(x, y) \mapsto (X, Y)$ of the plane F^2 but that whatever the choice of N, the identity

$$(X-1)(Y-1) = (x-1)(y-1)$$

means that, for each $\alpha \in F$, the hyperbola

$$H_\alpha = \{(x, y) : (x-1)(y-1) = \alpha\}$$

is transformed into itself.

Note also that the degenerate hyperbola H_0 is the union of

$$H_0^x = \{(x, y) : x = 1\} \quad \text{and} \quad H_0^y = \{(x, y) : y = 1\},$$

both of which are transformed into themselves under the above transformation for any choice of N.

We define a curve $L = ((x(s), y(s)) : s \in F)$ to be *special* if $(x(s)-1)(y(s)-1)$ is constant. Special curves have an important role in what follows.

Two particularly simple forms of tensor product are obtained by taking N to be the uniform matroid $U_{k,k+1}$ or $U_{1,k+1}$, with $k \geqslant 1$. (The *uniform matroid* $U_{r,n}$ has a ground set of n elements and bases all subsets of size r.) We call $M \otimes U_{k,k+1}$ the *k-stretch* of M and $M \otimes U_{1,k+1}$ the *k-thickening* of M. Note that since uniform matroids have transitive automorphism groups the choice of point to be distinguished is immaterial. Performing a k-stretch (respectively, k-thickening) on M amounts to replacing each of its elements by k elements in series (respectively, parallel).

If $\mathscr{C}$ is any class of matroids we say it is *closed under expansions* if for any $M \in \mathscr{C}$ and any positive integer k, both the k-stretch and k-thickening of M belong to $\mathscr{C}$.

Now in order to prove our two main results it is necessary not only that the classes of matroids under consideration are closed under expansions, but also that when the matroid is presented in its succinct representation the operations of k-stretch and k-thickening can be done in time which is polynomial both in k and in the size of the matroid, yielding a corresponding succinct representation of the new matroid.

Any class of matroids which is closed under expansions and polynomially closed in this sense is said to be *closed*. It is easy but tedious to check that all the classes of matroids used explicitly in this paper are closed.

We are (at last) in a position to state and prove our main results.

THEOREM 1. *Let $\mathscr{C}$ be a succinct closed class of matroids and let L be a rational curve in F^2. Then the problem $\pi_1[\mathscr{C}]$ of determining the Tutte polynomial on the plane for members of $\mathscr{C}$ is polynomial time reducible to the problem $\pi_3[\mathscr{C}, L]$ of evaluating the Tutte polynomial for members of $\mathscr{C}$ on the curve L, provided that L is not a special curve.*

In other words, determining the Tutte polynomial completely along a non-special curve is no easier than determining it in the whole plane.

Our second theorem relates evaluation along special curves with evaluation at a particular point.

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

In other words, apart from these *nine* points which we call *special points*, evaluating the Tutte polynomial at a point is no easier than evaluating it along the whole special curve containing the point. Since we will use this fact repeatedly we state it explicitly as follows:

COROLLARY. *For $\alpha \in F$, if $\pi_3[\mathscr{C}, H_\alpha]$ is #P-hard then $\pi_2[\mathscr{C}, a, b]$ is also #P-hard for any non-special point (a, b) of H_α.*

The proofs of Theorems 1 and 2 are rather technical and are postponed to Section 7.

5. *Examples and applications*

In this section we illustrate the applications of Theorems 1 and 2 by giving as complete a statement as we can of the computational difficulty of evaluating T at the special points and along the special curves.

Let $\mathscr{C}$ be a succinct closed class of matroids. We say that a point (a, b) (curve $L \subseteq F^2$) is *easy* for $\mathscr{C}$ if there is a polynomial time algorithm for the problem $\pi_2[\mathscr{C}, a, b]$ (respectively $\pi_3[\mathscr{C}, L]$). We similarly abuse notation by describing the point (curve) as #P-hard for $\mathscr{C}$ if the corresponding evaluation problem is #P-hard. We deal first with the special points.

(5·1) $(0, 0)$ is trivially easy for any class $\mathscr{C}$.

(5·2) $(1, 1)$ is the point where T counts the number of bases. This is easy for graphs by Kirchhoff's determinantal formula which has been extended to regular matroids but is not known to be easy for binary matroids.

(5·3) $(-1, -1)$ is easy for binary matroids by (2·8), but is #P-hard for the class of matroids coordinatizable over any other finite field except the field $\mathbb{F}_4$ of 4 elements, where it is also easy and is related to the bicycle dimension over $\mathbb{F}_4$ (see Vertigan [**44**]).

(5·4) $(0, -1)$ and $(-1, 0)$ are easy for binary matroids. This is because for a binary matroid $M = (S, \rho)$, $T(M; 0, -1)$ equals 0 if M has an odd cocycle and $(-1)^{|S|-\rho(S)}$

otherwise. For any other finite field different from $\mathbb{F}_2$, these points are $\#P$-hard for the class of matroids represented over this field (see [**44**]).

(5·5) The points (j, j^2) and (j^2, j) are easy for ternary matroids. This follows from Jaeger [**16**]. On the other hand we know from [**44**] that they are $\#P$-hard for the class of matroids representable over any other finite field.

(5·6) $(i, -i)$ and $(-i, i)$: We will present in the next section an interpretation at those points when M is the cycle matroid of a planar graph. This is in terms of the Arf invariant of a related alternating link. The evaluations are easy for binary matroids (but $\#P$-hard for the class of matroids representable over any other finite field) and are related to the binary bicycle space (see Vertigan [**44**]).

We now turn to the special curves. Recall that no other curve can be easy for any class $\mathscr{C}$ unless the complete determination of T is easy for that class.

(5·7) H_1: this is easy for any class $\mathscr{C}$ since by (2·15) along H_1, $T = x^n(x-1)^{r-n}$ where n is the size and r is the rank of the matroid.

(5·8) H_2: since this evaluation gives the Ising partition function, it is $\#P$-hard for the class of graphic matroids (Jerrum [**19**]), but easy for the class of planar graphs (the Ising problem can be reformulated in terms of perfect matchings: see Fisher [**9**] and Kasteleyn [**22**]).

(5·9) H_0^x is hard for cycle matroids of graphs since by (2·18) it corresponds to the calculation of the percolation probability (or reliability polynomial) of the graph which is $\#P$-hard by [**33**].

(5·10) H_0^y is hard for the class of planar graphic matroids. This follows from different independent arguments of Jerrum [**20**] and Vertigan [**44**].

(5·11) H_n, where n is an integer and $n \geqslant 3$, is $\#P$-hard for the class of graphic matroids since it contains the point $(1-n, 0)$ which corresponds by (2·12) to the counting of n-colourings, a known $\#P$-hard problem (see [**10**]).

(5·12) H_α for $\alpha \in F \setminus \mathbb{N}$: This special curve contains the point $(1-\alpha, 0)$. We shall show that this point is $\#P$-hard for cycle matroids of graphs. Consequently H_α is $\#P$-hard for the class of graphic matroids. Moreover, by the Corollary of Theorem 2, each of its points, being non-special is also $\#P$-hard for this class.

To show that $(1-\alpha, 0)$ is $\#P$-hard, we note that by (2·12) for any graph G, $T(M(G); 1-\alpha, 0)$ equals $P(G; \alpha)$ up to a simple factor. We now use an idea of Linial [**27**] to reduce polynomially the computation of $P(G; 3)$ to that of $P(G; \alpha)$.

Let $G + K_p$ be the graph obtained from G by adding p new vertices forming a clique K_p and adjacent to every vertex of G. Clearly

$$P(G + K_p; \lambda) = \lambda(\lambda-1)\dots(\lambda-p+1)P(G; \lambda-p).$$

Hence for every $\alpha \in F \setminus \mathbb{N}$ and $p \in \mathbb{N}$, $P(G; \alpha-p)$ can be computed in polynomial time from $P(G+K_p; \alpha)$. By doing this for $|V(G)|+1$ values of p we obtain $P(G; \lambda)$ for $|V(G)|+1$ distinct values of λ and since $P(G; \lambda)$ is a polynomial with maximum degree $|V(G)|$ this yields $P(G; \lambda)$ by Lagrange interpolation. The reduction is clearly a polynomial time reduction and this completes the proof of our assertion.

Thus we have a complete description of the complexity of the evaluation of the Tutte polynomial of graphic matroids which we sum up in the following proposition.

PROPOSITION 1. *If $\mathscr{C}$ is the class of graphic matroids, then the problem $\pi_2[\mathscr{C}; a, b]$ of evaluating the Tutte polynomial of a member of $\mathscr{C}$ at (a, b) is $\#P$-hard at any point of the*

set $F^2\backslash(H_1 \cup S)$, where S is the set of 9 special points listed in Theorem 2. On $F^2 \cap (H_1 \cup S)$ the problem of evaluating the Tutte polynomial is easy.

Proof. This follows immediately from (5·1)–(5·12) above and the Corollary to Theorem 2.

A Corollary of Proposition 1 is the following result.

PROPOSITION 2. *Counting nowhere-zero flows with values in Z_k in a graph is #P-hard for $k \geqslant 3$.*

Proof. This is because, by (2·13), the number of nowhere-zero flows with values in Z_k in a graph G is given (up to an easily determined constant) by $T(M(G); 0, 1-k)$ and since $(0, 1-k)$ is not special this is no easier than evaluating T along H_k, which we know to be $\#P$-hard for $k \geqslant 3$.

Note that for $k \geqslant 6$, by Seymour's theorem [**37**], the corresponding decision problem is trivial. Note also that by duality (see (2·3)) Proposition 1 holds with graphic replaced by cographic.

6. *Polynomials for knots and links*

Here is a brief outline of the relevant parts of knot theory. More details can be found in Kauffman [**23**] or Lickorish [**26**].

A *link* K with $c(K)$ components consists of $c(K)$ disjoint smooth simple closed curves embedded in three-dimensional space. A *knot* is a link with one component. A link is *oriented* if each component is assigned a direction. Two links are *equivalent* if there exists a continuous deformation of space (ambient isotopy) which transforms one onto the other.

It is well known (see for example [**23**] or [**26**]) that links can be represented as plane graphs in which each edge is assigned a positive or negative sign. An *alternating link* K is a link which can be represented by a plane graph $G(K)$ with all edges positive. In this case the Jones polynomial of K (provided with some orientation) can be expressed in terms of the Tutte polynomial of $G(K)$ as follows (see [**39**]).

(6·1) For an alternating oriented link K, the Jones polynomial of K is

$$V_K(t) = f_K(t)\, T(M(G(K)); -t, -1/t),$$

where $f_K(t)$ is an easily determined factor and is plus or minus a half integer power of t.

In other words the Jones polynomial of an alternating link is an evaluation of the Tutte polynomial of the corresponding planar graph along the hyperbola $xy = 1$. But we know from Theorem 1 that this is a $\#P$-hard curve for the class of planar graphs. Since every plane graph is easily seen to be of the form $G(K)$ for some alternating link K we have shown

THEOREM 3. *Determining the Jones polynomial of an alternating link is #P-hard.*

An immediate corollary is that determining any of the polynomials (such as the Kauffman or Homfly polynomial) which specialize to the Jones polynomial must also be $\#P$-hard. This strengthens the observation of Jaeger [**15**] which shows that determining the Homfly polynomial is NP-hard and the similar result of Thistlethwaite [**40**] that determining the Kauffman polynomial is NP-hard.

It is interesting also to consider Theorem 2 as applied to links. Suppose we wish to evaluate the Jones polynomial at a particular point, $t = a \neq 0$. Then we need to be able to evaluate T at the point $(-a, -1/a)$. This point lies on the special curve H_C where $C = (a+1)^2/a$. Except when a is one of the 8 values $1, -1, -j, -j^2, i, -i, j, j^2$, we know from Theorem 2 and the discussion in Section 5 that the problem is likely to be difficult. More precisely we have the following pessimistic result:

(6·2) evaluating the Jones polynomial $V_K(t)$ at $t = a$ for an alternating oriented link K is no easier than determining the Tutte polynomial of a planar graph along the hyperbola H_C unless a is $1, -1, -j, -j^2, i, -i$. (It is easy for $a = j$ or j^2, since then $(-a, -1/a)$ lies on H_1.)

At the particular special points which we have found there is already an interpretation of the Jones polynomial (see Lickorish [**26**]):

(6·3) $V_K(1) = (-2)^{c(K)-1}$ where $c(K)$ is the number of components of K.

(6·4) $V_K(-1) = \Delta_K(-1)$, where $\Delta_K(t)$ is the Alexander polynomial of K.

(6·5) $V_K(i) = (-\sqrt{2})^{c(K)-1}(-1)^{\mathrm{Arf}(K)}$ or 0 if $\mathrm{Arf}(K)$ is undefined, where $\mathrm{Arf}(K)$ is the *Arf invariant* of K (see [**26**]). If $\bar{K}$ is the mirror image of K then $V_K(-i) = V_{\bar{K}}(i)$.

(6·6) $V_K(-j^2) = \delta(K)\, i^{c(K)-1}(i\sqrt{3})^{d(D(K))}$, where $d(D(K))$ is the dimension of the first $\mathbb{F}_3$-homology of the double cyclic cover of S^3 branched along K and $\delta(K) = \pm 1$ is determined by Lipson [**28**]. Also $V_K(-j) = V_{\bar{K}}(-j^2)$.

(6·7) $V_K(j) = V_K(j^2) = 1$ for all K. (Note that when the number of components of K is even, $V_K(t)$ is actually $\sqrt{t}$ times a polynomial in t. The above values are based on one choice of root, and if the other is chosen, then multiply by $(-1)^{c(K)-1}$.)

All the above values are polynomially computable functions of the link K represented by its link diagram [**23**, **26**]. A realistic conjecture based on the above study of special points was the following.

(6·8) For any value of t other than $\pm 1, \pm i, \pm j, \pm j^2$ the evaluation of the Jones polynomial $V_K(t)$ of an alternating link is a $\#P$-hard problem.

This would follow immediately if Proposition 1 (with $H_1 \cup S$ replaced by $H_1 \cup H_2 \cup S$) held for the class of matroids of planar graphs. This turns out to be true but its proof is more involved (note that the techniques of (5·11), (5·12) fail for planar graphs) and is given in Vertigan [**44**].

7. *Proof of Theorems* 1 *and* 2

We turn now to the proof of our two main results. The basic idea in both cases involves using the tensor product of Brylawski [**6**]. For example, determining the Tutte polynomial of k-stretches or k-thickenings of a matroid M at a fixed non-special point (a, b) gives the Tutte polynomial of M at several points on the special curve containing (a, b). Using Lagrange interpolation this gives the polynomial along this curve. Despite the inherent simplicity of this main idea we see no way of avoiding some of the technicalities in what follows.

In what follows it will often be easier to work with the Whitney rank generating function R rather than the Tutte polynomial T. The transformation (4·1) becomes for $M = (S, \rho)$

$$R(M \otimes N; x, y) = R_C^{|S|-\rho(S)} R_L^{\rho(S)} R\left(M; \frac{xR_C}{R_L}, \frac{yR_L}{R_C}\right) \tag{7·1}$$

where R_C and R_L are abbreviations for $R_C(N; x, y)$ and $R_L(N; x, y)$, which like R are obtained from $T_C(N; x, y)$, $T_L(N; x, y)$ by the simple translation $R(x, y) = T(x+1, y+1)$.

In the special case where we are taking the k-stretch and k-thickening it is useful to note that the formulae (4·2) yield for the k-stretch

$$\left.\begin{aligned} T_C &= 1+x+\ldots+x^{k-1}, \quad T_L = 1, \\ R_C &= \frac{(x+1)^k-1}{x}, \quad R_L = 1, \end{aligned}\right\} \tag{7·2}$$

and for the k-thickening

$$\left.\begin{aligned} T_C &= 1, \quad T_L = 1+y+\ldots+y^{k-1}, \\ R_C &= 1, \quad R_L = \frac{(y+1)^k-1}{y}. \end{aligned}\right\} \tag{7·3}$$

Proof of Theorem 1. Let $M \in \mathscr{C}$ be a matroid of size n and consider the curve

$$L = \{(x(s), y(s)) : s \in F\}.$$

We will be working with the rank generating function R so we assume that $x(s)\,y(s)$ is not constant in order that the computation of R along L corresponds to the computation of T along a non-special curve. For the moment we assume also that $x(s)$ is not constant.

Let M' be the k-stretch of M, where k is a positive integer to be determined later. From the formulae (7·1)–(7·2) we know that

$$R(M'; x(s), y(s)) = \left[\frac{(x(s)+1)^k-1}{x(s)}\right]^{|S|-\rho(S)} R(M; X(s), Y(s)) \tag{7·4}$$

where

$$X(s) = (x(s)+1)^k-1, \quad Y(s) = x(s)\,y(s)/[(x(s)+1)^k-1]. \tag{7·5}$$

Write

$$\left.\begin{aligned} R(M; X(s), Y(s)) &= \sum_{i=0}^{n}\sum_{j=0}^{n} r_{ij} X(s)^i\, Y(s)^j = \sum_{i=0}^{n}\sum_{j=0}^{n} r_{ij} (X(s)\,Y(s))^j\, X(s)^{i-j} \\ &= \sum_{h=-n}^{n}\sum_{j} r_{h+j,j} (X(s)\,Y(s))^j\, X(s)^h \end{aligned}\right\} \tag{7·6}$$

by letting $h = i-j$ and where the second summation is over integers j such that $0 \leqslant j \leqslant n$, $0 \leqslant j+h \leqslant n$. Our purpose is to recover the coefficients r_{ij}.

Since L is a rational curve we can put

$$X(s)\,Y(s) = x(s)\,y(s) = \frac{u(s)}{v(s)},$$

and

$$X(s) = \frac{w(s)}{z(s)},$$

where the right-hand sides are rational functions expressed in standard form.

Then, for the moment ignoring the dependence on s,

$$R(M; X, Y) = \sum_{h=-n}^{n} \left(\sum_{j} r_{h+j,j} \left(\frac{u}{v}\right)^j\right)\left(\frac{w}{z}\right)^h = (vwz)^{-n} \sum_{h=-n}^{n} \left(\sum_{j} r_{h+j,j}\, u^j\, v^{n-j}\right) w^{n+h}\, z^{n-h}$$

and combining this with (7·4) and (7·6), if

$$t_h(s) = \sum_j r_{h+j,j}\, u(s)^j v(s)^{n-j} \quad (-n \leqslant h \leqslant n),$$

we obtain

$$\sum_{h=-n}^{n} t_h\, w^{n+h} z^{n-h} = (vwz)^n \left[\frac{(x+1)^k - 1}{x}\right]^{\rho(S)-|S|} R(M'; x, y). \tag{7·7}$$

We now present a polynomial time algorithm for determining the r_{ij} from knowledge of the Whitney rank generating function of M' on the curve L.

The rational functions $x(s), y(s)$ are given so the polynomials u, v are easily obtained, but w and z depend on the choice of k. The algorithm demands that the degree of either $w(s)$ or $z(s)$ is greater than that of any of the polynomials $t_h(s)$ $(-n \leqslant h \leqslant n)$.

If $x(s) = x_1(s)/x_2(s)$ is in standard form, it can be checked that

$$\max\{\deg(w), \deg(z)\} = k \max\{\deg(x_1), \deg(x_2)\}.$$

To see this simply put $w = (x_1 + x_2)^k - x_2^k$ and $z = x_2^k$ and then check that the above equality holds and that $w(s)/z(s)$ is a rational function in standard form (by the unique factorization property a common prime divisor of w and z would divide x_1 and x_2 so that w and z are relatively prime). Note also that the right-hand side is non-zero since $x(s)$ is not constant (by the initial hypothesis). Also

$$\max\{\deg(t_h) : -n \leqslant h \leqslant n\} \leqslant n \max\{\deg(u), \deg(v)\}$$

as follows immediately from the definition of t_h. Hence a sufficiently large k is easily found.

Once k is chosen, the polynomials $w(s)$ and $z(s)$ are easily found and the k-stretch M' of M easily constructed. Since $\mathscr{C}$ is closed under expansions, the algorithm applied to M' yields the rational expression $R(M'; x(s), y(s))$ and using (7·7), multiplication by suitable known polynomials yields the polynomial

$$A(s) = \sum_{h=-n}^{n} t_h(s)\, w(s)^{n+h} z(s)^{n-h}.$$

Without loss of generality we may assume (by symmetry) that $z(s)$ has degree greater than any $t_h(s)$. Now

$$t_n(s)\, w(s)^{2n} \equiv A(s) \bmod z(s),$$

and using the Euclidean algorithm the unique $\bar{w}(s) \in F[s]$ having degree less than that of $z(s)$ and satisfying

$$w(s)\, \bar{w}(s) \equiv 1 \bmod z(s)$$

is easily found. This gives $t_n(s)$ as the unique polynomial of degree less than that of z and such that

$$t_n(s) \equiv (\bar{w}(s))^{2n} A(s) \bmod z(s),$$

and again this is easily determined.

Subtracting $t_n(s)(w(s))^{2n}$ from $A(s)$ and dividing by $z(s)$ we repeat the procedure to find t_{n-1} and by repeated recursion the remaining t_h.

The same procedure is used to obtain the coefficients r_{ij} $(i, j = 0, 1, \ldots, n)$ from the

(now known) $t_h(s)$ $(-n \leqslant h \leqslant n)$. (Note that since the r_{ij} are constants and $x(s)y(s)$ is not, at least one of $u(s)$ and $v(s)$ has degree higher than that of every r_{ij}.)

It is routine (but tedious) to check that, apart from the one call to the oracle giving T on the curve L, the algorithm runs in polynomial time as required for a polynomial-time reduction. Hence the theorem is proved except for non-special curves L with $x(s)$ constant. But since the dual argument, using k-thickening instead of k-stretch, works for non-special curves except those with $y(s)$ constant, and since a non-special curve cannot have both $x(s)$ and $y(s)$ constant, the theorem is proved. ∎

We now turn to the proof of Theorem 2. First note that every special curve is contained in exactly one of H_α $(\alpha \in F \setminus \{0\})$ or H_0^x or H_0^y except for the trivial (degenerate) curve consisting of the single point $(1,1)$. Thus there is no loss of generality in regarding the special curve L as parametrized by

$$x(s) = s+1, \quad y(s) = \alpha/s+1 \quad (\alpha \in F, s \in F), \tag{7·8}$$

which means $L = H_\alpha$ when $\alpha \neq 0$ and $L = H_0^y$ when $\alpha = 0$.

(The line H_0^x is covered by dualizing the argument and any other special curve is obtained by reparametrizing s to some rational function of itself.)

We now define a point (a,b) to be *typical with respect to a class* $\mathscr{C}$ if with L_{ab} denoting the unique special curve (parametrized as above) through (a,b), the problem of evaluating the Tutte polynomial along L_{ab} for a member of $\mathscr{C}$ is Turing reducible to evaluating the Tutte polynomial at (a,b).

Proof of Theorem 2. We must show that (a,b) is typical with respect to a class $\mathscr{C}$ provided that it is not one of the nine points listed in the statement of Theorem 2.

Let $M \in \mathscr{C}$ have size n and note that

$$s^n T\left(M; s+1, \frac{\alpha}{s}+1\right) = s^n R(M; s, \alpha/s) = s^n \sum_{i=0}^{n} \sum_{j=0}^{n} r_{ij} s^{i-j} \alpha^j = \sum_{h=-n}^{n} r_h s^{n+h}$$

where

$$r_h = \sum_j r_{h+j,j} \alpha^j \quad (-n \leqslant h \leqslant n)$$

and where the summation is over integers j such that $0 \leqslant j \leqslant n$ and $0 \leqslant j+h \leqslant n$ as in the proof of Theorem 1.

Recall that we need to recover the coefficients r_h (this is what is meant by determining T along the curve L), and we will do this by determining T at $2n+1$ distinct points of L and using Lagrange interpolation.

Now if M' is the k-stretch of M, then by (4·1) and (7·2)

$$T(M'; a, b) = (1+a+\ldots+a^{k-1})^{n-\rho(M)} T\left(M; a^k, \frac{b+a+\ldots+a^{k-1}}{1+a+\ldots+a^{k-1}}\right).$$

Thus provided $1+a+\ldots+a^{k-1} \neq 0$ we can determine the Tutte polynomial of M at

$$x = a^k, \quad y = \frac{b+a+\ldots+a^{k-1}}{1+a+\ldots+a^{k-1}}$$

by constructing M' and calculating its Tutte polynomial at $(a,b) \in L$. Provided a is not zero or a root of unity then doing this for $k = 1, 2, \ldots, 2n+1$ gives values of $T(M; x, y)$ at $2n+1$ distinct points on L and hence determines it everywhere along

the curve. Thus (a, b) is typical. Similarly if b is not zero or a root of unity we can use the k-thickening rather than the k-stretch in the above argument and again (a, b) is typical.

Thus we have shown that if (a, b) is not typical then $|a| \in \{0, 1\}$ *and* $|b| \in \{0, 1\}$.

To complete the proof of the theorem we need to find stretch or thickening transformations of the plane sending the points in question to points already known to be typical. We now show how to achieve this.

Suppose that (a, b) *is not typical and* $|a| = |b| = 1$. Using the 2-stretch it follows that

$$\left(a^2, \frac{b+a}{1+a}\right)$$

is not typical or undefined. Thus $a = -1$ or

$$\left|\frac{b+a}{1+a}\right| \in \{0, 1\}.$$

This implies that $b = -a$ or $b = a^2$ or $b = 1$.

Using the 2-thickening it follows by a dual argument that $b = -1$ or $a = -b$ or $a = b^2$ or $a = 1$. The only possibilities are that

$$(a, b) \in \{(1, 1), (-1, -1), (j, j^2), (j^2, j), (-1, i), (-1, -i),$$
$$(i, -1), (-i, -1)\} \cup \{(a, -a) : |a| = 1\}.$$

By similarly applying the 3-stretch and 3-thickening one finds that only

$$(1, 1), (-1, -1), (j, j^2), (j^2, j), (i, -i) \quad \text{and} \quad (-i, i)$$

remain as possible atypical points of the form (a, b) where $|a| = |b| = 1$.

Suppose that $(a, 0)$ *is not typical.* Then $|a| \in \{0, 1\}$, and considering the 2-stretch, $(a^2, a/(1+a))$ is not typical or is undefined. Thus $a = -1$ or $a = 0$ or $|1+a| = 1$, the last possibility occurring only for $a \in \{0, j, j^2\}$. But $a \notin \{j, j^2\}$ since $(j^2, -j^2)$ and $(j, -j)$ are typical by the previous case. Thus the only possible atypical points of this form are $(0, 0)$ and $(-1, 0)$.

By duality the only possible atypical points of the form $(0, b)$ are $(0, 0)$ and $(0, -1)$ and hence we have reduced the set of possible atypical points to the set of nine points specified in the statement of Theorem 2. This completes the proof. ∎

The reason that this polynomial time reduction does not work for these nine special points is that the transformations associated to k-stretches and k-thickening send each of these points to finitely many other points. More specifically when the results of the transformations are defined, $(1, 1)$, $(0, 0)$, $(-1, -1)$, $(-1, 0)$ and $(0, -1)$ are sent to themselves, (j, j^2) and (j^2, j) are sent to (j, j^2) or (j^2, j), and $(i, -i)$ and $(-i, i)$ are sent to $(i, -i)$, $(-i, i)$, $(-1, 0)$ or $(0, -1)$.

The authors would like to acknowledge some very helpful conversations with Mark Jerrum, and also thank him for communicating his constructions mentioned in Section 5. The first author is partially supported by the PRC 'Mathématiques et Informatique'.

REFERENCES

[1] R. J. BAXTER. *Exactly Solved Models in Statistical Mechanics* (Academic Press, 1982).

[2] L. BERMAN and J. HARTMANIS. On isomorphisms and density of *NP* and other complete sets. *SIAM J. Comput.* **6** (1977), 305–321.

[3] J. A. BONDY and U. S. R. MURTY. *Graph Theory with Applications* (American Elsevier and Macmillan, 1976).

[4] T. H. BRYLAWSKI. A decomposition for combinatorial geometries. *Trans. Amer. Math. Soc.* **171** (1972), 235–282.

[5] T. H. BRYLAWSKI and D. LUCAS. Uniquely representable combinatorial geometries. In *Proceedings of International Colloquium in Combinatorial Theory, Rome, Italy, 1973; Atti Convegni Lincei* **17** (1976), 83–104.

[6] T. H. BRYLAWSKI. The Tutte polynomial; matroid theory and its applications. *Centro Internazionale Matematico Estivo* **3** (1980), 125–275.

[7] T. H. BRYLAWSKI and J. G. OXLEY. The Tutte polynomial and its applications. In *Matroid Theory*, vol. 3 (ed. N. White) (Cambridge University Press, to appear).

[8] H. CRAPO. The Tutte polynomial. *Aequationes Math.* **3** (1969), 211–229.

[9] M. E. FISHER. On the dimer solution of planar Ising models. *J. Math. Phys.* **7** (1966), 1776–1781.

[10] M. R. GAREY and D. S. JOHNSON. *Computers and Intractability – A Guide to the Theory of NP-completeness* (Freeman, 1979).

[11] M. R. GAREY, D. S. JOHNSON and L. STOCKMEYER. Some simplified *NP*-complete graph problems. *Theoret. Comput. Sci.* **1** (1976), 237–267.

[12] C. GREENE. Weight enumeration and the geometry of linear codes. *Stud. Appl. Math.* **99** (1976), 117–128.

[13] M. GRÖTSCHEL, L. LOVÁSZ and A. SCHRIJVER. *Geometric Algorithms and Combinatorial Optimization* (Springer-Verlag, 1988).

[14] F. JAEGER. On Tutte polynomials and cycles of plane graphs. *J. Combin. Theory Ser. B* **44** (1988), 129–146.

[15] F. JAEGER. On Tutte polynomials and link polynomials. *Proc. Amer. Math. Soc.* **103** (1988), 647–654.

[16] F. JAEGER. On Tutte polynomials and bicycle dimension of ternary matroids. *Proc. Amer. Math. Soc.* **107** (1989), 17–25.

[17] F. JAEGER. Nowhere zero flow problems. In *Selected Topics in Graph Theory 3* (ed. L. Beineke and R. J. Wilson) (Academic Press, 1988), pp. 71–95.

[18] M. R. JERRUM. The complexity of evaluating multivariate polynomials. Ph.D. thesis, University of Edinburgh (1981).

[19] M. R. JERRUM. 2-dimensional monomer-dimer systems are computationally intractable. *J. Statist. Phys.* **48** (1987), 121–134.

[20] M. JERRUM. (Private communication, March 1989.)

[21] V. F. R. JONES. A polynomial invariant for knots via Von Neumann algebras. *Bull. Amer. Math. Soc.* **12** (1985), 103–111.

[22] P. W. KASTELEYN. Graph theory and crystal physics. In *Graph Theory and Theoretical Physics* (ed. F. Harary) (Academic Press, 1967), pp. 43–110.

[23] L. KAUFFMAN. *On Knots* (Princeton University Press, 1987).

[24] M. LAS VERGNAS. Convexity in oriented matroids. *J. Combin. Theory Ser. B* **29** (1980), 231–243. Matroides orientables. *C. R. Acad. Sci. Paris Ser. A* **280** (1975), 61–64.

[25] M. LAS VERGNAS. Le polynôme de Martin d'un graphe Eulérien. *Ann. Discrete Math.* **17** (1983), 397–411.

[26] W. B. R. LICKORISH. Polynomials for links. *Bull. London Math. Soc.* **20** (1988), 558–588.

[27] N. LINIAL. Hard enumeration problems in geometry and combinatorics. *SIAM J. Algebraic Discrete Methods* **7** (1986), 331–335.

[28] A. S. LIPSON. An evaluation of a link polynomial. *Math. Proc. Cambridge Philos. Soc.* **100** (1986), 361–364.

[29] F. J. MACWILLIAMS and N. J. A. SLOANE. *The Theory of Error Correcting Codes* (North Holland, 1977).

[30] P. MARTIN. Remarkable valuation of the dichromatic polynomial of planar multigraphs. *J. Combin. Theory Ser. B* **24** (1978), 318–324.

[31] J. G. OXLEY and D. J. A. WELSH. The Tutte polynomial and percolation. In *Graph Theory and Related Topics* (Academic Press, 1979), pp. 329–339.

[32] J. S. PROVAN. The complexity of reliability computations in planar and acyclic graphs. *SIAM J. Comput.* **15** (1986), 694–702.
[33] J. S. PROVAN and M. O. BALL. The complexity of counting cuts and of computing the probability that a graph is connected. *SIAM J. Comput.* **12** (1983), 777–788.
[34] G. C. ROBINSON and D. J. A. WELSH. The computational complexity of matroid properties. *Math. Proc. Cambridge Philos. Soc.* **87** (1980), 29–45.
[35] P. ROSENSTIEHL and R. C. READ. On the principal edge tripartition of a graph. *Ann. Discrete Math.* **3** (1978), 195–226.
[36] P. D. SEYMOUR. Decomposition of regular matroids. *J. Combin. Theory Ser. B* **28** (1980), 305–359.
[37] P. D. SEYMOUR. Nowhere-zero 6-flows. *J. Combin. Theory Ser. B* **30** (1981), 130–135.
[38] R. P. STANLEY. *Enumerative Combinatorics*, vol. 1 (Wadsworth & Brooks/Cole, 1986).
[39] M. B. THISTLETHWAITE. A spanning tree expansion of the Jones polynomial. *Topology* **26** (1987), 297–309.
[40] M. B. THISTLETHWAITE. On the Kauffman polynomial of an adequate link. *Invent. Math.* **93** (1988), 285–296.
[41] W. T. TUTTE. A ring in graph theory. *Proc. Cambridge Philos. Soc.* **43** (1947), 26–40.
[42] L. G. VALIANT. The complexity of computing the permanent. *Theoret. Comput. Sci.* **8** (1979), 189–201.
[43] L. G. VALIANT. The complexity of enumeration and reliability problems. *SIAM J. Comput.* **8** (1979), 410–421.
[44] D. L. VERTIGAN. On the computational complexity of Tutte, Homfly and Kauffman invariants (to appear).
[45] D. J. A. WELSH. *Matroid Theory*. London Math. Soc. Monograph no. 8 (Academic Press, 1976).
[46] D. J. A. WELSH. Matroids and their applications. In *Selected Topics in Graph Theory 3* (ed. L. Beineke and R. J. Wilson) (Academic Press, 1988), pp. 43–71.
[47] H. WHITNEY. A logical expansion in mathematics. *Bull. Amer. Math. Soc.* **38** (1932), 572–579.
[48] H. WHITNEY. On the abstract properties of linear dependence. *Amer. J. Math.* **57** (1935), 509–533.
[49] T. ZASLAVSKY. Facing up to arrangements: face count formulas for partitions of spaces by hyperplanes. Memoirs Amer. Math. Soc. vol. 154 (American Mathematical Society, 1975).