Chromatic, Flow, and Reliability Polynomials: the Complexity of their Coefficients

James Oxley*
Department of Mathematics
Louisiana State University
Baton Rouge, Louisiana, 70803, USA

and

Dominic Welsh*
Mathematical Institute
University of Oxford
Oxford, OX1 3LB, UK

19 October 2001

Abstract

We study the complexity of computing the coefficients of three classical polynomials, namely the chromatic, flow and reliability polynomials of a graph. Each of these is a specialisation of the Tutte polynomial $\Sigma t_{ij} x^i y^j$. It is shown that, unless $NP = RP$, many of the relevant coefficients do not even have good randomised approximation schemes. We consider the quasiorder induced by approximation reducibility and highlight the pivotal position of the coefficient $t_{10} = t_{01}$, otherwise known as the beta invariant.

Our nonapproximability results are obtained by showing that various decision problems based on the coefficients are NP-hard. A study of such predicates shows a significant difference between the case of graphs, where, by Robertson-Seymour theory, they are in polynomial time, and matrices over finite fields, where they are shown to be NP-hard.

1 Introduction

Although the study of the complexity of counting problems is more than twenty years old, there are still far more questions unanswered than not. Here we concentrate on

*The authors were partially supported by, respectively, the National Security Agency and the ESPRIT Project RAND-APX.

counting problems arising in the study of classical combinatorial polynomials.

We assume familiarity with the chromatic and flow polynomials of a graph and the Tutte polynomial of a matroid; more details can be found in [12] or [40]. The basics of counting complexity such as the relation of $\#P$ to other complexity classes can be found in [40].

Throughout, Σ will denote a finite alphabet and Σ^* will be the language of finite strings of elements of Σ. For $x \in \Sigma^*$, its length is denoted by $|x|$. A *randomised approximation scheme* for a function $f : \Sigma^* \to \mathbb{N}$ is a randomised algorithm which takes as input a pair $(x, \varepsilon) \in \Sigma^* \times (0, 1)$ and produces as output an integer random variable Y satisfying

$$Pr\left\{\frac{1}{1+\varepsilon} \leq \frac{Y}{f(x)} \leq 1+\varepsilon\right\} \geq \frac{3}{4}.$$

It is a *fully polynomial* scheme if its running time is bounded by a polynomial in $|x|, \varepsilon^{-1}$. Such a scheme is often called an *fpras* (pronounced "effpras"). The following well-known observation about the existence of an fpras will be used frequently throughout the paper.

Lemma 1.1 *If $f : \Sigma^* \to \mathbb{N}$ is such that deciding whether f is non-zero is NP-hard, then there is no fpras for f unless $NP = RP$.*

Much of the time, we will be concerned with graphs. However, some of our results and problems extend naturally to matroids and, in particular, to the matroids arising from matrices with entries from a finite field. To accommodate this, we use the concept of an "accessible" matroid, defined precisely below.

In this paper, we will be addressing the problem of computing matroid invariants in time bounded by a polynomial in n, the size of the ground set of the matroid. In order for this to be even a sensible question, a first requirement is that it is possible to *describe* the matroid in time which is bounded by a polynomial function of n. We call classes of matroids which can be so described *succinct*; for a precise definition, see [24]. In practice, we are principally concerned with the succinct classes consisting of matroids obtained from graphs or from matrices with entries from some finite or algebraically closed field. Whether the matroid is described by a graph or by its matrix representation is immaterial as far as polynomial-time computations are concerned. Thus henceforth when we refer to a computational question for one of these classes of matroids, we will implicitly assume that the matroid will be given (or described) by a graph, by a matrix, or by some other such succinct presentation.

We say that a class $\mathcal{M}$ of matroids is *accessible* if

a) each member of $\mathcal{M}$ has a succinct representation;

b) if $M \in \mathcal{M}$, the rank of any subset of $E(M)$ can be found in time bounded by a polynomial in $|E(M)|$;

c) $\mathcal{M}$ is closed under minors and, from a succinct representation of $M \in \mathcal{M}$, it is possible to find a succinct representation of each deletion $M \backslash e$ and each contraction M/e in time which is bounded by a polynomial in $|E(M)|$.

For the relation between this and other oracle representations of matroids, we refer to Robinson and Welsh [35].

It is clear that many of the standard classes of matroids encountered in practice are accessible. More specifically:

1.2 *The classes of graphic and cographic matroids are accessible.*

1.3 *If $\mathcal{M}(F)$ denotes the class of matroids coordinatisable over a field F, then $\mathcal{M}(F)$ is accessible.*

All of the specific polynomials whose complexity is studied here are specialisations of the 2-variable Tutte polynomial $T(M; x, y)$. As far as *evaluations* of these polynomials are concerned, the problems of *deciding* their complexity are completely answered in the papers of [24] and [39]. In particular, it is known [39] that, even for a bipartite planar graph, every evaluation $T(G; a, b)$ is $\#P$-hard except when (a, b) lies on two particular curves or is one of 8 special points. Here we are principally concerned with individual coefficients of the various polynomials.

Where possible, we have separated the coefficients into those which are computable in polynomial time (p-time), and those which are $\#P$-hard. In the latter case, we have tried to show the existence of an fpras or prove that, barring some unlikely collapse in the complexity hierarchy, no fpras can exist.

The graph terminology is standard; the matroid terminology follows Oxley [31].

2 The chromatic and flow polynomials

When G is a graph with $k(G)$ components, its chromatic polynomial $P(G; \lambda)$ and flow polynomial $F(G; \lambda)$ have the form

$$P(G; \lambda) = a_1\lambda + a_2\lambda^2 + \cdots + a_n\lambda^n$$

and

$$F(G; \lambda) = f_0 + f_1\lambda + \cdots + f_d\lambda^d$$

where $n = |V(G)|$ and $d = |E(G)| - |V(G)| + k(G)$. Whereas both a_n and f_d are known to equal 1, at the other end of the range we have the following hardness result.

Proposition 2.1 *Even for bipartite planar graphs, the following problems are $\#P$-hard:*
a) computing a_k for any fixed $k \geq 1$,
b) computing f_k for any fixed $k \geq 0$.

Proof. Take G to be connected. Then

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

so

$$|a_1| = \lim_{\lambda \to 0} \left| \frac{P(G; \lambda)}{\lambda} \right| = T(G; 1, 0).$$

From [39], computing this evaluation of T is $\#P$-hard even for bipartite planar graphs.

To see that computing a_k is $\#P$-hard, note that if we take k vertex-disjoint copies of G and call the graph obtained $G^{(k)}$, then

$$P(G^{(k)}; \lambda) = (P(G, \lambda))^k.$$

Thus if there is a p-time algorithm to determine the coefficient of λ^k in $P(G^{(k)}; \lambda)$, we have a p-time algorithm for finding the coefficient of λ in $P(G; \lambda)$. But we have shown the latter to be $\#P$-hard.

To show that computing f_k is $\#P$-hard for any fixed $k \geq 0$, we proceed as follows. Let G be a connected plane graph, let G^* be its dual, and let G_2 be the graph that is obtained from G by inserting a degree-2 vertex into each edge of G. Then G_2 is a bipartite plane graph and

$$F(G_2; \lambda) = F(G; \lambda).$$

Moreover,

$$F(G; \lambda) = \lambda^{-1} P(G^*; \lambda).$$

Thus if there is a p-time algorithm to determine the coefficient of λ^k in $F(G_2; \lambda)$, we have a p-time algorithm for finding the coefficient of λ^{k+1} in $P(G^*; \lambda)$. Since G^* is an arbitrary connected plane graph, the latter is $\#P$-hard by (i), and (ii) follows. □

3 Combinatorial complexes

The f-vector of a polytope or complex lists the number of its faces of each dimension. This and the intimately related h-vector have been the subject of massive research effort, particularly for shellable complexes (see, for example, [6]).

A *complex* Δ on a finite set E is simply a collection of subsets which is closed under containment. The members of Δ are called *faces* or *simplices*. The *dimension* of Δ is the maximum cardinality of a face in Δ. (Note that this definition of dimension is one more than is often found in the literature, but it is much more natural in the context of combinatorics.) We say Δ is *pure* if every maximal face has the same cardinality d. These maximal faces are called *facets*.

A pure d-dimensional complex Δ is *shellable* if its facets can be ordered as B_1, $B_2, \dots, B_m$ such that, for all $k \in \{2, 3, \dots, m\}$,

$$P(B_k) \cap \bigcup_{i=1}^{k-1} P(B_i)$$

is a pure $(d-1)$-dimensional complex. Here $P(X)$ denotes the collection of subsets of X. A pure complex is *partitionable* if its faces can be partitioned into intervals $[L_1, U_1], [L_2, U_2], \dots, [L_p, U_p]$, where each U_i is a facet of Δ.

It is well-known that any shellable complex is partitionable and if

$$h_i = |\{j : |L_j| = i\}|,$$

then

$$h_k = \sum_{j=0}^{k} (-1)^{k-j} \left(\begin{array}{c} d-j \\ d-k \end{array} \right) f_j$$

where f_j is the number of faces of Δ of cardinality j. Thus $(f_0, f_1, ..., f_d)$ and $(h_0, h_1, ..., h_d)$ are related by writing

$$\begin{aligned} h(\Delta, x) &= \sum_{i=0}^{d} h_i x^i \quad \text{and} \\ f(\Delta, x) &= \sum_{i=0}^{d} f_i x^i \end{aligned}$$

to give

$$h(\Delta, x) = (1-x)^d f(\Delta, \frac{x}{1-x}). \tag{1}$$

Note 3.1 *Björner [6] uses the h_i in reverse order. Although this has some notational advantages, we prefer to stick with standard practice.*

Almost all the complexes we deal with henceforth are *matroid complexes*. Such a complex Δ is the complex of independent sets of a matroid $M = (E, r)$. The facets of Δ are the bases of M and the faces are the independent sets. Hence

$$f(\Delta, x) = \sum_{k=0}^{r} i_k x^k,$$

where i_k is the number of independent subsets of size k in M.

Every matroid complex is shellable and the h-vectors and f-vectors of matroid complexes have natural interpretations in terms of the Tutte polynomial which we now address.

4 The tableau of Tutte coefficients

The Tutte polynomial $T(M; x, y)$ of a matroid $M = (E, r)$ can be written in the two forms:

$$\begin{aligned} T(M; x, y) &= \sum_{A \subseteq E} (x-1)^{r(E)-r(A)} (y-1)^{|A|-r(A)} \qquad (2) \\ &= \sum_{i,j} t_{i,j} x^i y^j \end{aligned}$$

where each $t_{i,j}$ is a non-negative integer.

It is convenient to represent T as a tableau or $r+1$ by $(|E|-r)+1$ array as shown:

$$\begin{pmatrix} t_{0,0} & t_{0,1} & \dots & t_{0,|E|-r} \\ t_{1,0} & t_{1,1} & \dots & \\ \vdots & & & \\ t_{r,0} & & & \end{pmatrix}$$

We use R_i $(0 \leq i \leq r)$ and C_j $(0 \leq j \leq |E|-r)$ to denote the row and column sums, respectively, of the matrix $(t_{i,j})$. Thus

$$\sum_{i=0}^{r} R_i x^i = T(M;x,1)$$

and

$$\sum_{j=0}^{|E|-r} C_j y^j = T(M;1,y).$$

Putting $y=1$ in (2) shows that

$$\begin{aligned} T(M;x,1) &= \sum_{A \subseteq E:\ A \text{ independent}} (x-1)^{r(E)-|A|} \\ &= \sum_{k=0}^{r} i_k(M)(x-1)^{r-k}. \end{aligned}$$

Hence,

$$T(M;x,1) = (x-1)^r f(\Delta(M), \frac{1}{x-1}).$$

But, from (1),

$$h\left(\Delta, \frac{1}{x}\right) = \left(\frac{x-1}{x}\right)^r f\left(\Delta, \frac{1}{x-1}\right)$$

so

$$h\left(\Delta, \frac{1}{x}\right) = x^{-r} T(M;x,1)$$

giving for any matroid M, the identity

$$(h_r, h_{r-1}, ..., h_0) = (R_0, R_1, ..., R_r).$$

It follows from [39] that, even for bipartite planar graphs, computing the whole array $(t_{i,j})$ must be $\#P$-hard. Annan [4] makes this precise. We summarise his results as follows. The input in each case is a graph with n vertices and m edges.

4.1 *For fixed $(i,j) \neq (0,0)$, computing $t_{i,j}$ is $\#P$-complete.*

4.2 *For all fixed a and arbitrary i and j, computing*

$$t_{n-1-a,j} \quad \textit{and} \quad t_{i,m-n+1-a}$$

is in P.

4.3 *For a constant* α *with* $0 \leq \alpha < 1$*, computing*

$$t_{\lfloor \alpha n+1,0 \rfloor}$$

is $\#P$*-complete.*

4.4 *For a constant* c *with* $0 < c \leq 1$*, computing*

$$t_{\lfloor n-n^c+1 \rfloor,0}$$

is $\#P$*-complete.*

4.5 *Computing* $t_{\lfloor (n-1)/2 \rfloor, \lfloor (n-m+1)/2 \rfloor}$ *is* $\#P$*-complete.*

Loosely speaking, the combination of the above says that almost all the $t_{i,j}$ are $\#P$-hard except for those in a finite "South-East" border of the tableau.

On the positive side, it follows from Oxley and Welsh [32] that:

4.6 *For any* i, j*, computing* $t_{i,j}$ *is in* P *for series-parallel graphs and for any class of accessible matroids whose largest* 3*-connected member has bounded cardinality.*

Andrzejak [2] and Noble [29] have extended the graphical version of this and independently shown:

4.7 *For any* i, j*, computing* $t_{i,j}$ *is in* P *for any class of graphs of bounded tree width.*

We return to these coefficients in Sections 6 and 7. First we consider some questions about reliability.

5 Reliability polynomials

An enormous amount of effort has gone into the study of reliability polynomials and the F-vectors, and H-vectors which are associated with them (see, for example, Brown and Colbourn [8]).

First we give the basic definitions. Suppose that G is a connected graph and each edge is independently operating (or present) with probability p and not operating (or absent) with probability $1-p$. $\mathrm{Rel}(G, p)$ denotes the probability that the resulting subgraph of G is connected and is known as the (all-terminal) *reliability.* Standard forms for the reliability polynomial when G has m vertices and n edges are (see Brown and Colbourn [8])

$$\begin{aligned} \mathrm{Rel}(G,p) &= \sum_{i=0}^{m-n+1} F_i p^{m-i}(1-p)^i \\ &= \sum_{i=n-1}^{m} N_i p^i (1-p)^{m-i} \\ &= p^{n-1} \sum_{i=0}^{m-n+1} H_i (1-p)^i. \end{aligned}$$

Here F_i and N_i are, respectively, the number of independent sets of $M^*(G)$ of size i and the number of spanning connected subgraphs of G with i edges, and $\{H_i\}$ is the h-vector of $\Delta(M^*(G))$.

Clearly

5.1 *F_{m-n+1} is the number of spanning trees of G.*

5.2 *$F_0 = 1$ and F_1 is the number of edges of G that are not isthmuses.*

All of these are p-time computable and it is easy to see that the following is true.

5.3 *For any fixed k, computing F_k is in P.*

At the other end of the range, apart from (5.1), not much seems to be known. In [14], Chari and Colbourn pose the following problem which as far as we know is still open.

Problem 5.4 *Can the number of spanning connected unicyclic subgraphs of a graph be computed efficiently?*

The subgraphs we are seeking to count here correspond to spanning trees plus one edge. Liu and Chow [27] show there is a p-time algorithm for this problem in planar graphs. Interest in this seemingly strange problem is because the number sought is the next-to-leading coefficient in the f-expansion of the reliability polynomial. Curiously, it also arose in a completely different context in a problem of Przytycki [33] on the Jones polynomial of a knot.

Although the status of exact computation is still open, we do have:

Theorem 5.5 *(Annan [3]) For any fixed integer k, there exists an fpras for counting the number of spanning connected subgraphs with $n - 1 + k$ edges in a graph on n vertices.*

Turning to the H-form of the reliability polynomial, it is known (see, for example, [14]) that the following is true.

5.6 *For any fixed k, in a graph of edge connectivity c, there is a p-time algorithm to calculate $H_0, H_1, ..., H_{c+k}$.*

At the other end of the polynomial, one encounters the *reliability domination* $D(G)$ of a graph G. This is a parameter which has received a lot of attention in the literature (see, for example, Boesch et al [7]). It turns out that $D(G)$ is just the coefficient $H_{m-n+1}(G)$. Chari and Colbourn [14] note that, by a result of Vertigan [38], the computation of H_{m-n+1} is $\#P$-hard even for planar graphs. The next proposition extends this observation.

Proposition 5.7 *For any fixed $k \geq 0$, computing $H_{m-n+1-k}$ is $\#P$-hard even for planar graphs.*

Proof. For any connected graph G, we know that $\{H_i\}$ is the h-vector of $\Delta(M^*(G))$. Hence

$$\begin{aligned}\sum H_k z^k &= h(\Delta(M^*(G)); z) \\ &= z^{r(M^*(G))} T(M^*(G); z^{-1}, 1) \\ &= z^{|E|-r(M(G))} T(G; 1, z^{-1}) \\ &= \sum C_{m-n+1-k} z^k\end{aligned}$$

where C_j is the j-th column sum of the Tutte tableau of G. Thus it suffices to show that computing C_k is $\#P$-hard. To see this, suppose that G' is obtained from the input graph G by adding a single loop. Then

$$T(G'; x, y) = yT(G; x, y).$$

Putting $x = 1$ and rewriting in terms of the column sums $\{C_k\}$ gives, by comparing coefficients, $C_k(G') = C_{k-1}(G)$. Hence, for any fixed $k > 0$, a p-time algorithm to compute C_k gives a p-time algorithm for C_{k-1}. Iterating this gives a p-time algorithm for computing $C_0 = H_{m-n+1}$ which we know to be $\#P$-hard for planar connected graphs.

□

6 Approximations

Now we turn to the question of which of the above coefficients have good approximation schemes. First we show that, unless there is a surprising collapse of complexity hierarchies, there can be no fpras for "most" of the coefficients $t_{i,j}$.

Proposition 6.1 *Unless $NP = RP$, there is no fpras for the following:*
Input: *Connected graph G on n vertices and rational ϵ in $(0, 1)$.*
Output: *Coefficient $t_{i,j}$ for*

$$i = n - \lfloor n^\epsilon \rfloor, \quad j = \binom{\lfloor n^\epsilon \rfloor - 1}{2}.$$

Proof. Leo [26] proves that, when $k \geq 3$ and $M = M(G)$ is simple,

$$t_{r(M)-k+1, n(k)}$$

counts the number of subgraphs of G which are k-cliques. Here

$$n(k) = \binom{k-1}{2}.$$

Now it is easy to prove that deciding whether a connected n-vertex graph contains a clique of size $\lfloor n^\epsilon \rfloor$ is NP-complete. The idea is to start with a version of clique known to be NP-complete, such as the existence of an $(n/2)$-clique. Then augment the input G by adding m isolated vertices to get G' where m is chosen so that G' on N vertices has an N^ϵ-clique if and only if G has an $(n/2)$-clique. Existence of an fpras for the counting problem would give an RP-algorithm for the decision problem and hence imply $NP = RP$. □

Following [19], if $f, g : \Sigma^* \to \mathbb{N}$ are functions whose complexity of approximation we wish to compare, an *approximation preserving reduction* from f to g is a probabilistic oracle Turing machine M which takes as input a pair $(x, \varepsilon) \in \Sigma^* \times (0, 1)$ and satisfies (i)–(iii) below:

(i) every oracle call made by M is of the form (ω, δ) where $\omega \in \Sigma^*$ is an instance of g and $\delta \in (0, 1)$ is an error bound satisfying

$$\delta^{-1} \leq p(|x|, \varepsilon^{-1})$$

where p is a fixed polynomial;

(ii) the Turing machine M meets the specification of being a randomised approximation scheme for f whenever the oracle meets the specification for being a randomised approximation scheme for g;

(iii) the run time of M is polynomial in $|x|$ and ε^{-1}.

When such an approximation preserving reduction exists, we write $f \leq_{AP} g$ and say f is *AP-reducible* to g.

In other words, if π_1 and π_2 are two counting problems, we say π_1 is *approximation reducible* or *AP-reducible* to π_2 if the existence of an fpras for π_2 implies the existence of an fpras for π_1. We should emphasise that, although this definition appears quite forbidding, all the reductions which we will be using are of a very straightforward character. A first easy result is the following.

Proposition 6.2 *For fixed $i, j \geq 0$, if $\pi(t_{i,j})$ denotes the problem of computing the coefficient $t_{i,j}$, then*

$$\begin{array}{ll} (a) & \pi(t_{i,j}) \leq_{AP} \pi(t_{i+1,j}), \\ (b) & \pi(t_{i,j}) \leq_{AP} \pi(t_{i,j+1}). \end{array}$$

Proof.

$$T(M \oplus U_{1,1}; x, y) = xT(M; x, y)$$

so

$$t_{i+1,j}(M \oplus U_{1,1}) = t_{i,j}(M),$$

and this gives (a). A dual argument gives (b). □

Combining the above propositions shows that, for all the coefficients $t_{i,j}$ which are not on the *North-West fringe* of the tableau, there can be no fpras unless $NP = RP$. It also highlights the following question as one which is most in need of a clear answer.

Question 6.3 *Is there an fpras to estimate* $t_{1,0}$*?*

The reasons for this are that, from Proposition 6.2, a negative answer implies a negative answer for every coefficient $t_{i,j}$, while, as our next result shows, a positive answer gives a solution to the long-standing open question of whether there is an fpras for the number of acyclic orientations of a graph.

Proposition 6.4 *If* $a(G)$ *denotes the number of acyclic orientations of* G*, then*

$$\pi(a(G)) \leq_{AP} \pi(t_{1,0}).$$

Proof. Consider a connected graph G. Form G^+ by adding a new vertex joined to all vertices of G. Then

$$P(G^+;\lambda) = \lambda P(G;\lambda - 1).$$

Hence

$$(-\lambda)T(G^+;1-\lambda,0) = \lambda(\lambda-1)T(G;2-\lambda,0)$$

giving

$$T(G^+;x,0) = xT(G;x+1,0). \tag{3}$$

Comparing coefficients gives

$$t_{1,0}(G^+) = t_{1,0}(G) + t_{2,0}(G) + \cdots .$$

This gives an AP-reduction showing that

$$\pi(T(G;1,0)) \leq_{AP} \pi(t_{1,0}). \tag{4}$$

But putting $x=1$ in (3) shows that

$$\pi(T(G;2,0)) \leq_{AP} \pi(T(G;1,0))$$

and, since $T(G;2,0)$ counts acyclic orientations, the result follows. □

Extending the argument above as x runs through the integers shows that, for each positive integer k, the following is true:

$$\pi(T(G;k+1,0)) \leq_{AP} \pi(T(G;k,0). \tag{5}$$

Since, for any matroid, $t_{1,0} = t_{0,1}$, it is tempting to believe that the answer to the following question is positive.

Question 6.5 *Is it true that* $\pi(T(G;0,1)) \leq_{AP} \pi(t_{1,0})$?

Recall from §2 that $T(G;1,0)$ and $T(G;0,1)$ are, up to a sign, the coefficients a_1 and f_0, respectively, of the chromatic and flow polynomials. Hence another corollary of the above proof is:

$$\pi(a_1) \leq_{AP} \pi(t_{1,0}) \tag{6}$$

and Question 6.5 is equivalent to:

Question 6.6 *Is it true that* $\pi(f_0) \leq_{AP} \pi(t_{1,0})$?

A question which is prompted by the above is: What is the relationship between the problems of approximating coefficients "along the diagonal" $i + j = c$ for some constant c? In particular, we pose:

Question 6.7 *How do the difficulties of* $\pi(t_{1,1})$ *and* $\pi(t_{2,0})$ *compare?*

Another question in the same vein is based on the intuition that "diagonal distance" from $t_{0,0}$ provides a rough measure of the difficulty in computing $t_{i,j}$. Thus we pose:

Question 6.8 *Are the following statements true?*
a) $\pi(t_{0,2}) \leq_{AP} \pi(t_{2,1})$.
b) $\pi(t_{2,0}) \leq_{AP} \pi(t_{1,2})$.

Note, for the class of all matroids, or indeed any subclass closed under duality, these two statements are equivalent.

7 Polynomial time predicates

From the above, it is likely that good approximations to the coefficients a_1 and f_0 either do not exist or are going to be very hard to find. However, what we do have is the following:

Theorem 7.1 *The following questions about an input graph G and fixed positive integer k can be tested in polynomial time:*

a) For the coefficient a_1 of λ in $P(G;\lambda)$, is $|a_1|$ less than k?

b) For the constant term f_0 of $F(G,\lambda)$, is $|f_0|$ less than k?

c) Is h_d, the leading coefficient of the h-vector of a graphic or cographic matroid, less than or equal to k?

d) For fixed rational α and input p with $0 < p < 1$, is

$$\mathit{Rel}(G,p) \leq \alpha p^{n-1}(1-p)^{m-n+1}$$

for a graph with m edges and n vertices?

Annan [4] has shown that, for given fixed integers i, j, k, the predicate "$t_{i,j}(G)$ is less than k" can be decided in p-time. This result does not seem to imply the above or our next result which includes (a) to (d) as special cases.

Theorem 7.2 *For given non-negative rationals a, b, k, deciding whether*

$$T(M(G);a,b) \leq k$$

is in P.

Proof. Let $\pi = \pi(a, b, k)$ be the predicate "$T(M(G); a, b) \leq k$". For a matroid M with components $M_1, M_2, \ldots, M_p$, we know

$$T(M; a, b) = \prod_i T(M_i; a, b).$$

Since k is fixed, it is not hard to see that we can decide π in p-time for all a, b, k, if we can decide it for connected matroids in p-time.

Call a graph G such that $M(G)$ is connected a block. Consider the set of blocks G such that $\pi(a, b, k)$ holds for G and let $\mathcal{F}_k(a, b)$ consist of all minors of such blocks. Clearly $\mathcal{F}_k(a, b)$ is a minor-closed family.

We now assert that every graph $H \in \mathcal{F}_k(a, b)$ satisfies π. Suppose not. Then clearly H is not a block but must be a minor of some block G which does satisfy π. But, from Brylawski [10, Corollary 6.9], we know that if N is a minor of a connected matroid M, then, for each i, j,

$$t_{i,j}(N) \leq t_{i,j}(M).$$

But, since G is a block, $M(G)$ is connected and we have the contradiction

$$\begin{aligned} k &< T(M(H); a, b) \\ &\leq T(M(G); a, b) \leq k. \end{aligned}$$

To complete the proof, we observe that, by Robertson-Seymour theory [34], there are only a finite number of minor-minimal graphs which do not belong to $\mathcal{F}_k(a, b)$ for any non-negative k, a, b. Thus, given any block G, we can test membership in $\mathcal{F}_k(a, b)$ in $O(n^3)$ time and this completes the proof. □

The proof above depends heavily on the Robertson-Seymour theory of graph minors. We would like to extend the results to matrices, or more explicitly, to the class of accessible matroids. Despite the recent breakthrough by Geelen, Gerards and Whittle [22], there is as yet no algorithmic theory for matrix minors and consequently any proof will be more complicated.

Consider the following complexity question.

ACCESSIBLE(a, b, k).
Input: Accessible matroid M, fixed non-negative rationals a, b, k.
Question: Is $T(M; a, b) \leq k$?

Proposition 7.3 *For $a \geq 1$ and $b \geq 1$, there is a p-time algorithm for ACCESSIBLE(a, b, k).*

Proof. Dinolt [18] and Murty [28] established that an n-element connected matroid of rank r has at least $r(n-r)+1$ bases. Using this and the fact that $T(M; 1, 1)$ counts the number of bases of M, it is straightforward to show that if M is a matroid without loops or coloops, then $T(M; 1, 1) \geq |E(M)|$. Now let M be a matroid whose sets of loops and coloops are L and L^*, respectively. Then $T(M; 1, 1) = T(M \backslash (L \cup L^*); 1, 1)$.

If $M\backslash(L \cup L^*)$ has more than k elements, then, since $a \geq 1$ and $b \geq 1$, we have $T(M; a, b) \geq T(M; 1, 1) > k$. If $M\backslash(L \cup L^*)$ has fewer than k elements, then there are a bounded number of choices for $M\backslash(L \cup L^*)$ and so the problem of determining whether $T(M; a, b) \leq k$ has been reduced to checking a bounded number of cases. □

We cannot see how to extend this result to the case where a or b lies in $(0, 1)$. In particular, we cannot settle the cases $(a, b) = (0, 1)$ and $(a, b) = (1, 0)$ which correspond to $|f_0|$ and $|a_1|$ in the case of graphs.

In the same vein, we feel it should be possible to extend Annan's result from graphs to accessible matroids. In other words, we believe that the following is true.

Conjecture 7.4 *For fixed integers $i, j, k \geq 0$, there is a p-time algorithm to decide, for an accessible matroid M, whether or not $t_{i,j}(M) \leq k$.*

In an attempt to make progress on some of these problems, in the next section, we study in detail the special case $t_{1,0} = t_{0,1}$. This is the parameter $\beta(M)$, already much studied in the literature.

8 The beta invariant

The *beta invariant* $\beta(M)$ of a non-empty matroid M is the coefficient of x in the Tutte polynomial of M. Thus, when M is a loop or a coloop, $\beta(M)$ is 0 or 1, respectively. Crapo [15] proved the following:

Theorem 8.1 *Let M be a non-empty matroid.*

(i) If $e \in E(M)$ and e is neither a loop nor a coloop of M, then

$$\beta(M) = \beta(M\backslash e) + \beta(M/e).$$

(ii) If $|E(M)| \geq 2$, then

(a) $\beta(M) > 0$ if and only if M is connected; and

(b) $\beta(M^*) = \beta(M)$.

Exact excluded-minor conditions for β to take specific low values have been given by Oxley [30]. In the context of this paper, it is interesting to note two particular interpretations of β in terms of orientations of a graph.

Greene and Zaslavsky [23] have proved that, when M is the cycle matroid of a graph G,

8.2 *$\beta(M)$ counts the number of acyclic orientations of G in which i is the only source and j is the only sink, irrespective of the choice of an edge ij of G.*

Equivalently:

8.3 *If e is an edge of G, then $\beta(M)$ counts the number of acyclic orientations of G which become totally cyclic when the direction of e is switched.*

As we have shown, approximating β is at least as hard as approximating the number of acyclic orientations of G, and it is mildly surprising therefore to observe that Bubley and Dyer [13] have found an fpras for counting sink-free orientations which runs in time $O^*(n^2m^3 + n^5m)$.

Whether or not there is an fpras for determining β remains one of the most intriguing problems in this area. However, the main purpose of this section is to prove:

Theorem 8.4 *If $\mathcal{M}$ is an accessible class of matroids and k is a fixed integer, then, for $M \in \mathcal{M}$, it can be determined in polynomial time whether $\beta(M) < k$.*

In order to prove Theorem 8.4, we shall need some preliminaries. The wheel with r spokes and the whirl of rank r are denoted by $\mathcal{W}_r$ and $\mathcal{W}^r$, respectively. The next result is due to Crapo [15].

Lemma 8.5 *$\beta(M(\mathcal{W}_r)) = r - 1$ and $\beta(\mathcal{W}^r) = r$ for all $r \geq 2$.*

The following result extends an observation of Oxley [30, p. 274].

Lemma 8.6 *Suppose $k \geq 2$ and let M be a 3-connected matroid having $\beta(M) = k$. Then $|E(M)| \leq 2k + 2$. Moreover, equality holds if and only if $M \cong M(\mathcal{W}_{k+1})$.*

Proof. If $k = 2$, then, as M is 3-connected, it follows by [30, Theorem 2.2] that M is isomorphic to $M(\mathcal{W}_3)$ or $U_{2,4}$. Thus $|E(M)| \leq 6 = 2k + 2$ and equality holds if and only if $M \cong M(\mathcal{W}_{k+1})$. Hence the lemma holds for $k = 2$. Assume it holds for all integers k in $\{2, 3, \ldots, m - 1\}$ and let $k = m$. Now either

(i) M has an element e such that $M \backslash e$ or M/e is 3-connected, or

(ii) for all elements e of M, neither $M \backslash e$ nor M/e is 3-connected.

In the second case, by Tutte's Wheels-and-Whirls Theorem [36, 8.2], M is a wheel or a whirl. Since $\beta(M) = m$, it follows that $M \cong M(\mathcal{W}_{m+1})$ or $M \cong \mathcal{W}^m$. Thus $|E(M)| \leq 2m + 2$ with equality holding if and only if $M \cong M(\mathcal{W}_{m+1})$.

Now assume that (i) holds. Then $M \backslash e$ or $M^* \backslash e$ is 3-connected. By switching to the dual if necessary, we may assume that $M \backslash e$ is 3-connected. Since M/e must be connected, $\beta(M/e)$ is positive. Thus, as $\beta(M) = \beta(M \backslash e) + \beta(M/e)$, it follows that $\beta(M \backslash e) \leq m - 1$. Therefore, by the induction assumption, $|E(M \backslash e)| \leq 2(m - 1) + 2$. Hence $|E(M)| \leq 2m + 1$. The lemma follows by induction. $\square$

For all $n \geq 2$, let $\mathcal{B}_n$ be the set of minor-minimal matroids M for which $\beta(M) = n$. Let $\mathcal{B}_\infty = \cup_{n \geq 2} \mathcal{B}_n$. A basic tool in the proof of Theorem 8.4 is the following result of Cunningham and Edmonds [17] that every connected matroid has a unique decomposition into circuits, cocircuits, and 3-connected matroids with at least four elements.

Theorem 8.7 *Let M be a connected matroid. Then, for some positive integer k, there is a collection $M_1, M_2, \ldots, M_k$ of matroids and a k-vertex tree T with edges labelled $e_1, e_2, \ldots, e_{k-1}$ and vertices labelled $M_1, M_2, \ldots, M_k$ such that* *(i) each M_i is 3-connected or is a circuit or cocircuit;*

(ii) $E(M_1) \cup E(M_2) \cup \ldots \cup E(M_k) = E(M) \cup \{e_1, e_2, \ldots, e_k\}$;

(iii) if the edge e_i joins the vertices M_{j_1} and M_{j_2}, then $E(M_{j_1}) \cap E(M_{j_2})$ is $\{e_i\}$;

(iv) if no edge joins the vertices M_{j_1} and M_{j_2}, then $E(M_{j_1}) \cap E(M_{j_i})$ is empty;

(v) T does not have two adjacent vertices that are both labelled by circuits or that are both labelled by cocircuits.

Moreover, M is the matroid that labels the single vertex of the tree $T/e_1, e_2, \ldots, e_{k-1}$ at the conclusion of the following process: contract the edges $e_1, e_2, \ldots, e_{k-1}$ of T one by one in order; when e_i is contracted, its ends are identified and the vertex formed by this identification is labelled by the 2-sum of the matroids that previously labelled the ends of e_i. Furthermore, the tree T is unique to within relabelling of its edges.

The fact that the tree T in this theorem is unique comes at a price: one cannot insist, as one would like, that each M_i is 3-connected, for a big circuit or cocircuit can be decomposed in several ways into 3-element (and hence 3-connected) circuits or cocircuits, respectively. Cunningham and Edmonds also proved a variant of the last theorem in which (i) was replaced by the requirement that each M_i is 3-connected. In that case, one must eliminate (v) and the conclusion that T is unique, but otherwise the theorem remains intact. An important consequence of this variant is that, although T itself need not be unique, for each element e of M, the isomorphism type of the matroid that contains e in the decomposition is determined. We shall refer to a decomposition of M according to this variant of Theorem 8.7 as a *3-connected tree decomposition of M*. The decomposition whose existence is asserted in Theorem 8.7 will be called the *unique tree decomposition of M*. An element of a connected matroid is in a circuit or cocircuit in the unique tree decomposition of M if and only if it is in a circuit or cocircuit in some or, equivalently, all 3-connected tree decompositions of M.

Theorem 8.8 *The following statements are equivalent for a matroid M.*

(i) M is in $\mathcal{B}_\infty$.

(ii) M is connected, $|E(M)| \geq 3$, and, in the unique tree decomposition of M, no element of M is in either a circuit or a cocircuit in the tree decomposition.

(iii) M is connected, $|E(M)| \geq 3$, and, if T is some 3-connected tree decomposition of M, then no element of M is in either a circuit or a cocircuit of T.

This theorem follows immediately by combining the next two lemmas. The first of these is a consequence of Theorem 8.1 and the straightforward details are omitted.

Lemma 8.9 *A matroid M is in $\mathcal{B}_\infty$ if and only if $|E(M)| \geq 3$ and, for all elements e of M, both $M\backslash e$ and M/e are connected.*

The next result is well-known but we include the proof for completeness. There is a technical difficulty that arises in the proof, namely that one may be faced with taking a 2-sum in which one of the matroids has just two elements, an operation which is undefined. However, this problem is easily overcome by extending the definition of 2-sum to include the case when the matroids have two elements. In that case, the 2-sum of matroids N_1 and N_2 is, as usual, the parallel connection of N_1 and N_2 with the basepoint deleted.

Lemma 8.10 *Let e be an element of a connected matroid M with $|E(M)| \geq 3$. Then*

(i) $M\backslash e$ is disconnected if and only if e is in a circuit in the unique tree decomposition of M; and

(ii) M/e is disconnected if and only if e is in a cocircuit in the unique tree decomposition of M.

Proof. By duality, it suffices to prove (i). Let M_i be the matroid that contains e in the unique tree decomposition of M. Suppose that M_i is not a circuit. Then M_i is either a cocircuit or a 3-connected matroid. Thus $M_i\backslash e$ is connected. It follows that $M\backslash e$ is connected since the 2-sum of connected matroids is connected. On the other hand, if M_i is a circuit, then, as $|E(M_i)| \geq 3$, it follows that $M_i\backslash e$ is disconnected and so $M\backslash e$ is disconnected. □

Theorem 8.11 *Let $n \geq 2$ and M be a member of $\mathcal{B}_n$. Then $|E(M)| \leq 2n+2$. Moreover, equality holds if and only if*

(i) $M \cong M(\mathcal{W}_{n+1})$, or

(ii) $n = 4$ and M is the 2-sum of two copies of $M(K_4)$.

Proof. If M is 3-connected, then the theorem holds by Lemma 8.6. Thus we may assume that M is not 3-connected. Let $M_1, M_2, \ldots, M_m$ be the 3-connected matroids that label vertices in the unique tree decomposition of M and that are not circuits and are not cocircuits. Then, by Theorem 8.8, every element of M is in some M_i and every M_i contains a basepoint that is not in M. Thus

$$\begin{aligned} |E(M)| &\leq \sum_{i=1}^{m}(|E(M_i)| - 1) &(7)\\ &\leq \sum_{i=1}^{m}(2\beta(M_i) + 2 - 1) &(8)\\ &\leq [2\sum_{i=1}^{m}\beta(M_i) + (m-2)] + 2. &(9)\end{aligned}$$

Now if N_1 and N_2 are matroids, then $\beta(N_1 \oplus_2 N_2) = \beta(N_1)\beta(N_2)$ [30, p. 270]. Hence, as $\beta(M) = n$, we deduce that $\prod_{i=1}^{m}\beta(M_i) = n$. Thus the desired bound on $|E(M)|$ holds provided

$$\sum_{i=1}^{m}\beta(M_i) + \frac{m-2}{2} \leq \prod_{i=1}^{m}\beta(M_i). \qquad (10)$$

Without loss of generality, we may assume that

$$\beta(M_1) \geq \beta(M_2) \geq \ldots \geq \beta(M_m) \geq 2,$$

where the last inequality follows since every 3-connected matroid that is not a circuit or a cocircuit has $\beta \geq 2$ [9, Theorem 7.6]. Since $\sum_{i=1}^{m} \beta(M_i) + \frac{m-2}{2} \leq m\beta(M_1) + \frac{m-2}{2}$ and $2^{m-1}\beta(M_1) \leq \prod_{i=1}^{m} \beta(M_i)$, it follows that (10) holds provided

$$m\beta(M_1) + \frac{m-2}{2} \leq 2^{m-1}\beta(M_1).$$

This holds if and only if

$$\frac{m-2}{2} \leq (2^{m-1} - m)\beta(M_1).$$

The last inequality certainly holds for $m \geq 2$ and is strict for $m \geq 3$. But we know that $m \geq 2$. Therefore, when M is not 3-connected, $|E(M)| \leq 2n + 2$. Moreover, equality can only hold if $m = 2$ and equality holds in (10) and (8). Now equality in (10) implies that $\beta(M_1) = \beta(M_2) = 2$, and equality in (8) implies, by Lemma 8.6, that both M_1 and M_2 are isomorphic to $M(K_4)$. Since, for $M \cong M(K_4) \oplus_2 M(K_4)$, we have $|E(M)| = 10 = 2\beta(M) + 2$, we conclude that the matroids attaining equality in the bound in the theorem are as specified there. $\square$

We now turn to the proof of the main result of this section, Theorem 8.4. Note that the second paragraph of the next proof is very similar to the first part of the proof of Theorem 2 of [32].

Proof of Theorem 8.4. We may assume that k is positive since $\beta(M) \geq 0$ for all matroids M. For $k \geq 3$, every minor-minimal matroid N with $\beta(N) = i$ and $2 \leq i < k$ is in $\cup_{i=2}^{k-1} \mathcal{B}_i$. By Theorem 8.11, every matroid in this collection has at most $2k$ elements. Thus the number of matroids in $\cup_{i=2}^{k-1} \mathcal{B}_i$ equals $f(k)$ for some function f. To determine whether $\beta(M) < k$, we shall produce, from M, a minor-minimal matroid M' for which $\beta(M') = \beta(M)$. We then need only to compare M' with each of the $f(k)$ members of $\cup_{i=2}^{k-1} \mathcal{B}_i$ to determine whether $2 \leq \beta(M) < k$. The procedure used to produce M' will also enable us to determine whether $\beta(M) \in \{0, 1\}$.

By using the algorithm of Bixby and Cunningham [5], we may determine whether or not M is 3-connected and, if not, the algorithm will produce a 2-separation of M. Moreover, since the matroid is accessible, this can be done in time that is bounded by a polynomial in $|E(M)| = n$. This is because the main component of the algorithm involves using Edmonds' matroid intersection algorithm, which can be done in polynomial time for accessible matroids. By at most $n - 1$ applications of Bixby and Cunningham's algorithm, we obtain a decomposition of M into its connected components and, for each such component, we obtain a 3-connected tree decomposition. Note that when we find a 2-separation $\{S_1, S_2\}$ of a connected matroid N, we can obtain two matroids N_1 and N_2 of which N is the 2-sum as follows:

(i) For each i in $\{1, 2\}$, construct a basis B_i for $N|S_i$. Then, as $|B_1| + |B_2| = r(S_1) + r(S_2) = r(N) + 1$, the set $B_1 \cup B_2$ contains a circuit C of N, and C must meet both B_1 and B_2.

(ii) Let p_1 be an element of $C \cap B_2$, let p_2 be an element of $C \cap B_1$ and, for each i in $\{1, 2\}$, let $N_i = [N|(S_i \cup C)].(S_i \cup p_i)$. Then N is the 2-sum of N_1 and N_2 with respect to the basepoints p_1 and p_2, respectively.

If M has more than one component, then $\beta(M) = 0 < k$. Thus we may assume that M is connected. We may also assume that $|E(M)| > 1$ otherwise we can easily determine $\beta(M)$ exactly. Now consider the collection of matroids labelling the vertices in the tree decomposition obtained for M. From this collection, discard all circuits and all cocircuits, leaving a collection $M_{i_1}, M_{i_2}, \ldots, M_{i_m}$ of 3-connected matroids each with at least four elements. Then $\beta(M) = 1$ if and only if this collection is empty. If the collection is non-empty, then $\beta(M) = \prod_{j=1}^{m} \beta(M_{i_j})$. Now let M' be the matroid that is formed from a circuit with elements $e_1, e_2, \ldots, e_m$ by, for each j in $\{1, 2, \ldots, m\}$, attaching M_{i_j} at e_j via a 2-sum, where the basepoint of this 2-sum in M_{i_j} is arbitrarily chosen. Although M' will certainly depend on the choices of these basepoints, the value of $\beta(M')$ will not since $\beta(M') = \prod_{j=1}^{m} \beta(M_{i_j}) = \beta(M)$. Moreover, by Theorem 8.8, every proper minor of M' has a smaller value of β. Consider $|E(M')|$. By Theorem 8.11, if $|E(M')| \geq 2k + 1$, then $\beta(M') \geq k$. Thus we may assume that $|E(M')| \leq 2k$. Evidently $\beta(M) < k$ if and only if M' is isomorphic to one of the $f(k)$ members of $\cup_{i=2}^{k-1} \mathcal{B}_i$. □

9 Some Decision Problems

We have seen in Proposition 6.1 that knowing that it is, in some provable sense, hard to decide whether $t_{i,j} > 0$ is very strong evidence that there is no fpras for that $t_{i,j}$. Accordingly, in this section, we study various decision problems of this kind. First we state a positive result.

Theorem 9.1 *If $\mathcal{M}$ is an accessible class of matroids and i is a fixed positive integer, then, for $M \in \mathcal{M}$, there are p-time algorithms to detemine whether or not $t_{i,0}(M) = 0$ and whether or not $t_{0,i}(M) = 0$.*

Proof. By duality, it suffices to prove that such a p-time algorithm exists to determine whether or not $t_{i,0}(M) = 0$. Let $|E(M)| = n$. By at most $n - 1$ applications of Bixby and Cunningham's algorithm, we obtain a decomposition of M into its connected components. We can then check in p-time whether or not M has any loops. If M does have a loop, then $t_{i,0}(M) = 0$. Thus we may assume that M has no loops. Evidently we can determine in p-time both the rank r and the number k of components of M. Then, from a result of Brylawski [11, p. 222], $t_{i,0}(M) = 0$ if and only if $i \notin \{k, k+1, \ldots, r\}$. The theorem follows immediately. □

In contrast we have the following negative result.

Theorem 9.2 *Let i, j, and k be fixed positive integers. There is no function f in $\mathbb{Z}[x]$ such that, for every n-element matroid M, it can be determined by using at most $f(n)$ probes of an independence oracle whether or not $t_{i,j}(M) < k$.*

The proof will use two lemmas. The first combines results of Brylawski [11, p. 212] and Leo [26]. The *two-wheel* is the cycle matroid of the wheel graph with two spokes.

Lemma 9.3 *The following statements are equivalent for a connected matroid M.*

(i) $t_{1,1} > 0$.

(ii) M *is not uniform.*

(iii) M *has a two-wheel as a minor.*

The next lemma follows from a result of Brylawski [10, Corollary 7.14].

Lemma 9.4 *Suppose that r and $n-r$ are positive integers. Then*

$$\beta(U_{r,n}) = \binom{n-2}{r-1}.$$

Let r and n be integers exceeding one and m be a non-negative integer such that $r+m \le n$. Let $M(r,m,n)$ be the matroid that is obtained from $U_{r,n-m}$ by choosing a hyperplane X of the latter and freely adding m points to X to form the set H. In particular, $M(r,0,n) \cong U_{r,n}$ and $M(r,m,r+m) \cong U_{r-1,r-1+m} \oplus U_{1,1}$. It is clear that $M(r,m,n)$ is representable over the rationals and hence over the reals.

Lemma 9.5 *Let r and n be integers exceeding one and m be a non-negative integer such that $r+m \le n$. Then*

$$t_{1,1}(M(r,m,n)) = \binom{r-3+m}{r-2}.$$

Proof. First suppose that $n = r+m$. Clearly $t_{1,1}(M(r,m,r+m)) = t_{1,1}(U_{r-1,r-1+m} \oplus U_{1,1}) = t_{0,1}(U_{r-1,r-1+m})$. If $m > 0$, then $t_{0,1}(U_{r-1,r-1+m}) = \beta(U_{r-1,r-1+m}) = \binom{r-3+m}{r-2}$, where the last equality follows by Lemma 9.4. If $m = 0$, then $U_{r-1,r-1+m}$ is the direct sum of $r-1$ coloops, so $t_{0,1}(U_{r-1,r-1+m}) = 0$ and $t_{1,1}(M(r,m,r+m)) = 0 = \binom{r-3}{r-2}$.

Now assume that $r+m < n$. Choose an element e of $E(M(r,m,n)) - H$. Then $M(r,m,n)/e \cong U_{r-1,n-1}$ and $M(r,m,n)\backslash e \cong M(r,m,n-1)$. By Lemma 9.3, $t_{1,1}(U_{r-1,n-1}) = 0$, so $t_{1,1}(M(r,m,n)) = t_{1,1}(M(r,m,n-1))$. By repeating this process, we deduce that $t_{1,1}(M(r,m,n)) = t_{1,1}(M(r,m,r+m)) = \binom{r-3+m}{r-2}$. □

Proof of Theorem 9.2. For a matroid M, let M' be obtained by taking the direct sum of M with $i-1$ coloops and $j-1$ loops. Then $t_{i,j}(M') = t_{1,1}(M)$. It follows that it suffices to prove the theorem in the case that $i = j = 1$.

By Lemma 9.5, $t_{1,1}(M(r,s,2r)) = \binom{r-3+s}{r-2}$. Thus $t_{1,1}(M(r,0,2r)) = 0$, while $t_{1,1}(M(r,2,2r)) = r-1$. But $M(r,0,2r) \cong U_{r,2r}$, while $M(r,2,2r)$ differs from $U_{r,2r}$ in that the former has an $(r+1)$-element subset H of its ground set such that every r-element subset of H is a non-basis of the former but a basis of the latter. To detect the difference between $M(r,0,2r)$ and $M(r,2,2r)$ on a $(2r)-$element set E, we need to probe at least one r-element subset of each $(r+1)$-element subset of E to determine whether or not it is independent. Each r-element subset of E is in exactly r subsets of E of cardinality $r+1$. Thus at least $\frac{1}{r}\binom{2r}{r}$ probes of an independence oracle are needed to distinguish between $M(r,0,2r)$ and $M(r,2,2r)$. But, for $r>k$, we have $t_{1,1}(M(r,0,2r))=0$ while $t_{1,1}(M(r,2,2r))\geq k$. The theorem follows. $\square$

Suppose now we consider the following matrix problems.

TUTTE COEFFICIENT OVER FIELD F

Input: Matrix A with entries from the finite field F_q or the rationals $\mathbb{Q}$ and positive integers i,j.

Question: If $M=M[A]$, is $t_{i,j}(M)>0$?

The same argument that was used to prove Proposition 6.1 also shows that, as it stands, the above problem is NP-hard. This is because we allow i,j to be part of the input. For fixed i,j, this argument fails. On the other hand, Theorem 9.2 gives strong evidence that TUTTE COEFFICIENT is not in P. However, it is not a proof because the algorithmic steps which we are allowing are in terms of independence-oracle probes. Accordingly we next define:

UNIFORM MATROID ISOMORPHISM

Input: $k\times n$ matrix A with integer entries.

Question: Is $M[A]$ isomorphic to $U_{k,n}$?

Then we obtain the following result from Lemma 9.3.

Theorem 9.6 *Deciding whether $t_{1,1}(M[A])>0$ when A is an integer matrix is Turing equivalent to UNIFORM MATROID ISOMORPHISM.*

To the best of our knowledge, none of the classical "isomorphism" questions in combinatorics has been proved to be NP-hard nor are they known to be in P. Hence, initially, we suspected that UNIFORM MATROID ISOMORPHISM is another problem in the complexity gap. However, this is not the case, for Khachiyan [25] has shown that it is NP-hard to determine if a set of n rational points in d dimensions is affinely or linearly dependent. As immediate consequences of this fact and the last theorem, we have the following:

Theorem 9.7 *UNIFORM MATROID ISOMORPHISM is NP-hard.*

Corollary 9.8 *For an integer matrix A, deciding whether $t_{1,1}(M[A])>0$ is NP-hard.*

It follows from the last result and Lemma 1.1 that, for an integer matrix A, there can be no fpras for $t_{1,1}(M[A])$ unless $NP=RP$. However, when A is a matrix over a finite field F_q, the situation is quite different since, for any fixed q and sufficiently large n, the matroid $M[A]$ cannot be uniform.

We close this section with a result which shows that deciding whether $t_{1,w}(M)>0$ for a general accessible matroid is NP-hard. We do this by proving it hard for matrices with entries from a finite field. Whether a similar result holds for matrices over the rationals is not clear.

Theorem 9.9 *The following problem is NP-hard for any finite field F_q:*

Input: Matrix A with entries from F_q and positive integer w.

Question: Is $t_{1,w}(M[A]) > 0$?

Proof. From [12, p. 182], we know that the minimum distance $d(\mathcal{C})$ of a linear code $\mathcal{C}$ over F_q is obtainable from $T(M(\mathcal{C}))$ using the formula

$$d(\mathcal{C}) = n - r + 1 - \delta$$

where $\mathcal{C}$ has length n and dimension r, and

$$\delta = \max\{j : t_{i,j} > 0 \text{ for some } i > 0\}.$$

But we know from standard properties of the Tutte tableau (see, for example, [11, Proposition 6.5]) that, for a connected matroid, if $t_{i,j} > 0$, then $t_{k,l} > 0$ for all $(k,l) \neq (0,0)$ such that $0 \leq k \leq i$ and $0 \leq l \leq j$. Hence

$$\delta = \max\{j : t_{1,j} > 0\}.$$

Thus we have reduced the problem to finding the minimum distance of a linear code over F_q and, by the recent result of Vardy [37], we know this is NP-hard for all prime powers q. □

Note 9.10 *(i) We cannot replace an F_q-representable matroid by a graphic matroid (or even a regular matroid) in the above statement.*

(ii) By Lemma 1.1, the last theorem implies that, unless $NP = RP$, there is no fpras for $t_{1,w}$ for general integer w, even in the binary case.

10 Conclusion: an fpras order

We close with a brief overview. Define a quasi-order on Tutte invariants by $\mu < \lambda$ if the existence of an fpras for λ implies the existence of an fpras for μ; in other words, we are abbreviating the relation $\leq_{AP}$ of AP-reducibility to just $<$. Then, restricting attention to graphic inputs, we have from (4), (5), (6), and Proposition 6.2, that this quasi-order has the following structure, where $a(G) = T(G; 2, 0)$ denotes the number of acyclic orientations of G:

$$
\begin{array}{ccccccccccccc}
t_{3,0} & & & & t_{2,1} & & & & t_{1,2} & & & & t_{0,3} \\
& \diagdown & & \diagup & & \diagdown & & \diagup & & \diagdown & & \diagup & \\
& & t_{2,0} & & & & t_{1,1} & & & & t_{0,2} & & \\
& & & \diagdown & & & | & & & \diagup & & & \\
& & & & t_{1,0} & = & \beta & = & t_{0,1} & & & & \\
& & & & & & | & & & & & & \\
& & & & & & a_1(G) & & & & & & \\
& & & & & & | & & & & & & \\
& & & & & & a(G) & & & & & & \\
& & & & & & | & & & & & & \\
& & & & & & T(3,0) & & & & & & \\
& & & & & & | & & & & & & \\
& & & & & & T(4,0) & & & & & & \\
& & & & & & \vdots & & & & & &
\end{array}
$$

Of course, the whole order may significantly collapse if all the $t_{i,j}$ have an fpras. However, it does highlight the pivotal position of the invariant β. Deciding whether or not it has an fpras would be a significant advance.

The results of Section 9 show that the situation illustrated in the quasi-order above is significantly different when working in the class of matroids rather than graphs. In particular, for a matrix A over the rationals, we know from Lemma 1.1, Proposition 6.2, and Corollary 9.8 that, for i and j both positive, there is no fpras for $t_{i,j}(M[A])$ unless $NP = RP$.

We have also made no further progress on deciding how well the constant term f_0 of the flow polynomial can be approximated. Although duality arguments suggest it should be comparable in difficulty to approximating the coefficients of the chromatic polynomial and thus AP-reducible to $t_{1,0}$, we have not been able to prove this. We should also note that because $|f_0(G)| = |T(G;0,1)|$ and, by [1], the latter has an fpras for the class of dense graphs, then so does $|f_0(G)|$. There is no known comparable result for the coefficients of the chromatic polynomial.

Acknowledgement

The authors are very grateful to Marc Noy for drawing their attention to the paper of Khachiyan [25].

References

[1] N. Alon, A.M. Frieze and D.J.A. Welsh, Polynomial time randomised approximation schemes for Tutte-Grothendieck invariants: the dense case, *Random Structures Algorithms* **6** (1995), 459–478.

[2] A. Andrzejak, An algorithm for the Tutte polynomials of graphs of bounded treewidth, *Discrete Math.* **190** (1998), 39–54.

[3] J.D. Annan, D.Phil. Thesis, University of Oxford, 1994.

[4] J.D. Annan, The complexities of the coefficients of the Tutte polynomial, *Discrete Appl. Math.* **57** (1995), 93–103.

[5] R.E. Bixby and W.H. Cunningham, Matroids, graphs, and 3-connectivity, in *Graph Theory and Related Topics*, J.A. Bondy and U.S.R. Murty, eds., Academic Press, New York, 1979, pp. 91–103.

[6] A. Björner, The homology and shellability of matroids and geometric lattices, in *Matroid Applications*, N. White ed., Cambridge University Press, Cambridge, 1992, pp. 226–283.

[7] F.T. Boesch, A. Satyanarayana and C.L. Suffel, Least reliable networks and the reliability domination, *IEEE Trans. Comm.* **38** (1990), 2004–2009.

[8] J.I. Brown and C.J. Colbourn, Non-Stanley bounds for network reliability, *J. Algebraic Combinatorics* **5** (1996), 13–36.

[9] T.H. Brylawski, A combinatorial model for series-parallel networks, *Trans. Amer. Math. Soc.* **154** (1971), 1–22.

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

[11] T.H. Brylawski, The Tutte polynomial Part I: General theory, in: *Matroid Theory and Its Applications*, A. Barlotti, ed., Liguori, Naples, 1980, pp. 125–275.

[12] T.H. Brylawski and J.G. Oxley, The Tutte polynomial and its applications, in *Matroid Applications*, N. White, ed., Cambridge University Press, Cambridge, 1992, pp. 123–225.

[13] R. Bubley and M. Dyer, Graph orientations with no sink and an approximation for a hard case of #SAT, Proc. Eighth Annual ACM-SIAM Symposium on Discrete Algorithms (1997), 248–257.

[14] M. Chari and C.J. Colbourn, Reliability polynomials: a survey, *J. Combin. Inform. System Sci.* **22** (1997), 177–193.

[15] H.H. Crapo, A higher invariant for matroids, *J. Combin. Theory* **2** (1967), 406–417.

[16] W.H. Cunningham, *A combinatorial decomposition theory*, Ph. D. thesis, University of Waterloo, 1973.

[17] W.H. Cunningham and J. Edmonds, A combinatorial decomposition theory, *Canad. J. Math.* **32** (1980), 734–765.

[18] G.W. Dinolt, An extremal problem for non-separable matroids, *Théorie des Matroïdes*, C.P. Bruter, ed., Lecture Notes in Math. **211**, Springer-Verlag, Berlin, 1971, pp. 31–49.

[19] M. Dyer, L.A. Goldberg, C. Greenhill and M. Jerrum, On the relative complexity of approximate counting problems, in *Approximation Algorithms for Combinatorial Optimisation*, K. Jensen and S. Khuller eds., APPROX 2000, Lecture Notes in Computer Science **1913**, Springer, Berlin, 2000, pp. 108–120.

[20] E. Ehrhart, *Polynômes Arithmétiques et Méthodes des Polyédres en Combinatoire*, Birkhäuser, Basel, 1977.

[21] M.R. Garey and D.S. Johnson, *Computers and Intractability — A guide to the theory of NP-completeness*, W.H. Freeman, San Francisco, 1979.

[22] J.F. Geelen, A.M.H. Gerards and G. Whittle, Branch width and well-quasi-ordering in matroids and graphs (preprint July 11, 2000).

[23] C. Greene and T. Zaslavsky, On the interpretation of Whitney numbers through arrangements of hyperplanes, zonotopes, non-Radon partitions and orientations of graphs, *Trans. Amer. Math. Soc.* **280** (1983), 97–126.

[24] F. Jaeger, D.L. Vertigan and D.J.A. Welsh, On the computational complexity of the Jones and Tutte polynomials. *Math. Proc. Cambridge Philos. Soc.* **108** (1990), 35–53.

[25] L. Khachiyan, On the complexity of approximating extremal determinants in matrices, *J. Complexity* **11** (1995), 138–153.

[26] J.W. Leo, The coefficients of the Tutte polynomial, *Discrete Math.* **184** (1998), 121–135.

[27] C.I. Liu and Y. Chow, Enumeration of connected spanning subgraphs of a planar graph, *Acta Mathematica Hungarica* **41** (1983), 27–36.

[28] U.S.R. Murty, On the number of bases of a matroid, Proc. Second Louisiana Conf. on Combinatorics, Louisiana State University, Baton Rouge, 1971, pp. 387–410.

[29] S. Noble, Evaluating the Tutte polynomial for graphs of bounded tree-width, *Combin. Probab. Comput.* **7** (1998), 307–322.

[30] J.G. Oxley, On Crapo's beta invariant for matroids, *Stud. Appl. Math.* **66** (1982), 267–277.

[31] J.G. Oxley, *Matroid Theory*, Oxford Univ. Press, New York, 1992.

[32] J.G. Oxley and Welsh, D.J.A., Tutte polynomials computable in polynomial time, *Discrete Math.* **109** (1992), 185–192.

[33] J. Przytycki, private communication (1993).

[34] N. Robertson and P.D. Seymour, Graph Minors. II. Algorithmic aspects of tree width, *J. Algorithms* **7** (1986), 309–322.

[35] G.C. Robinson and D.J.A. Welsh, The computational complexity of matroid properties, *Math. Proc. Cambridge Philos. Soc.* **87** (1980), 29–45.

[36] W.T. Tutte, Connectivity in matroids, *Canad. J. Math.* **18** (1966), 1301–1324.

[37] A. Vardy, The intractability of computing the minimum distance of a code, *IEEE Trans. Inform. Theory* **43** (1997), 1757–1766.

[38] D.L. Vertigan, *On the computational complexity of Tutte, Jones, HOMFLY and Kauffman invariants*, D.Phil. thesis, University of Oxford, 1991.

[39] 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.

[40] D.J.A. Welsh, *Complexity: Knots, Colourings and Counting*, London Math. Soc. Lecture Notes **186**, Cambridge University Press, Cambridge, 1993.

[41] D.J.A. Welsh, Randomised approximation in the Tutte plane, *Combin. Probab. Comput.* **3** (1994), 137–143.