Polynomial time randomised approximation schemes for Tutte-Gröthendieck invariants: the dense case

Noga Alon* Alan Frieze† Dominic Welsh‡

Abstract

The Tutte-Gröthendieck polynomial $T(G; x, y)$ of a graph G encodes numerous interesting combinatorial quantities associated with the graph. Its evaluation in various points in the (x, y) plane give the number of spanning forests of the graph, the number of its strongly connected orientations, the number of its proper k-colorings, the (all terminal) reliability probability of the graph, and various other invariants the exact computation of each of which is well known to be $\#P$-hard. Here we develop a general technique that supplies fully polynomial randomised approximation schemes for approximating the value of $T(G; x, y)$ for any dense graph G, that is, any graph on n vertices whose minimum degree is $\Omega(n)$, whenever $x \geq 1$ and $y > 1$, and in various additional points. Annan [2] has dealt with the case $y = 1$, $x \geq 1$. This region includes evaluations of reliability and partition functions of the ferromagnetic Q-state Potts model. Extensions to linear matroids where T specialises to the weight enumerator of linear codes are considered as well.

1 Introduction

Consider the following very simple counting problems associated with a graph G.

(i) What is the number of connected subgraphs of G?

(ii) How many subgraphs of G are forests?

(iii) How many acyclic orientations has G?

*Department of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel. Email: noga@math.tau.ac.il. Research supported in part by a USA-Israeli BSF grant and by the Fund for Basic Research administered by the Israel Academy of Sciences.

†Department of Mathematics, Carnegie Mellon University, Pittsburgh PA15213, U.S.A., Supported by NSF grant CCR-9225008

‡Merton College and Mathematical Institute, Oxford, UK. Research supported in part by ESPRIT RAND.

Each of these is a special case of the general problem of evaluating the Tutte polynomial of a graph (or matroid) at a particular point of the (x, y)-plane — in other words is a Tutte-Gröthendieck invariant. Other invariants include:

(iv) the chromatic and flow polynomials of a graph;

(v) the partition function of a Q-state Potts model;

(vi) the Jones polynomial of an alternating link;

(vii) the weight enumerator of a linear code over $GF(q)$.

It has been shown in Vertigan and Welsh [19] that apart from a few special points and 2 special hyperbolae, the exact evaluation of any such invariant is $\#P$-hard even for the very restricted class of planar bipartite graphs. However the question of which points have a fully polynomial randomised approximation scheme (*fpras*) is wide open. A survey of what is currently known is given in [21]. Here we prove several new results concerning the existence of a fpras for *dense* graphs. More precisely, for $0 < \alpha < 1$, let $\mathcal{G}_\alpha$ denote the set of graphs $G = (V, E)$ with $|V| = n$ and minimum degree $\delta(G) \geq \alpha n$. A graph is α-dense if it is a member of $\mathcal{G}_\alpha$ or, somewhat loosely, dense if we omit the α.

Various counting and approximation problems are known to be easier for graphs of sufficiently high density than for general graphs. The number of perfect matchings in bipartite graphs (which is *not* an evaluation of the Tutte polynomial) is one such example. The results of Broder [3] and of Jerrum and Sinclair [10] supply a fpras for approximating that number for (1/4)-dense bipartite graphs. Dyer, Frieze and Jerrum [5] found an fpras for the number of Hamilton cycles in graphs which are α-dense when $\alpha > 1/2$. Annan [2] obtained a fpras for the number of forests of a dense graph (given by the value of the Tutte polynomial at $(2, 1)$). Edwards [6] showed that the number of proper k colorings of sufficiently dense graphs (given by evaluating the Tutte polynomial at $(1-k, 0)$) can be computed exactly in polynomial time, whereas it is clear that this number cannot be approximated in polynomial time for general graphs unless $RP = NP$.

Our main new result is a general technique that supplies fully polynomial randomised approximation schemes for approximating the value of $T(G; x, y)$ for any dense graph G, whenever $x \geq 1$ and $y > 1$, and in various additional points. Annan [2] has dealt with the case $y = 1$, $x \geq 1$.

The graph terminology used is standard. The complexity theory and notation follows Garey and Johnson [8]. The matroid terminology follows Oxley [13]. Further details of most of the concepts treated here can be found in Welsh [20].

2 Tutte-Gröthendieck invariants

First consider the following recursive definition of the function $T(G; x, y)$ of a graph G, and two independent variables x, y.

If G has no edges then $T(G; x, y) = 1$, otherwise for any $e \in E(G)$;

(2.1) $T(G; x, y) = T(G'_e; x, y) + T(G''_e; x, y)$ if e is neither a loop nor an isthmus, where G'_e denotes the deletion of the edge e from G and G''_e denotes the contraction of e in G,

(2.2) $T(G; x, y) = xT(G'_e; x, y)$ e an isthmus,

(2.3) $T(G; x, y) = yT(G''_e; x, y)$ e a loop.

From this, it is easy to show by induction that T is a 2-variable polynomial in x, y, which we call the *Tutte polynomial* of G.

In other words, T may be calculated recursively by choosing the edges in *any* order and repeatedly using (2.1-3) to evaluate T. The remarkable fact is that T is well defined in the sense that the resulting polynomial is independent of the order in which the edges are chosen.

Alternatively, and this is often the easiest way to prove properties of T, we can show that T has the following expansion.

First recall that if $A \subseteq E(G)$, the *rank* of A, $r(A)$ is defined by

$$r(A) = |V(G)| - k(A),$$

where $k(A)$ is the number of connected components of the graph having vertex set $V = V(G)$ and edge set A.

It is now straightforward to prove:

The Tutte polynomial $T(G;x,y)$ can be expressed in the form

$$T(G;x,y) = \sum_{A \subseteq E} (x-1)^{r(E)-r(A)}(y-1)^{|A|-r(A)}.$$

These ideas can be extended to matroids - see for example [4] and [20].

3 A catalogue of invariants

We now collect together some of the naturally occurring interpretations of the Tutte polynomial. Throughout G is a graph, M is a matroid and E will denote $E(G), E(M)$ respectively.

(3.1) At (1,1) T counts the number of bases of M (spanning trees in a connected graph).

(3.2) At (2,1) T counts the number of independent sets of M, (forests in a graph).

(3.3) At (1,2) T counts the number of spanning sets of M, that is sets which contain a base.

(3.4) At (2,0), T counts the number of acyclic orientations of G. Stanley [17] also gives interpretations of T at $(m,0)$ for general positive integer m, in terms of acyclic orientations.

(3.5) Another interpretation at (2,0), and this for a different class of matroids, was discovered by Zaslavsky [23]. This is in terms of counting the number of different arrangements of sets of hyperplanes in n-dimensional Euclidean space.

(3.6) $T(G;-1,-1) = (-1)^{|E|}(-2)^{d(B)}$ where B is the bicycle space of G, see Read and Rosenstiehl [15]. When G is planar it also has interpretations in terms of the Arf invariant of the associated knot.

(3.7) The chromatic polynomial $P(G;\lambda)$ is given by

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

where $k(G)$ is the number of connected components.

(3.8) The flow polynomial $F(G;\lambda)$ is given by

$$F(G;\lambda) = (-1)^{|E|-r(E)}T(G;0,1-\lambda).$$

(3.9) The (all terminal) reliability $R(G;p)$ is given by

$$R(G;p) = q^{|E|-r(E)} p^{r(E)} T(G;1,1/q)$$

where $q = 1 - p$.

In each of the above cases, the interesting quantity (on the left hand side) is given (up to an easily determined term) by an evaluation of the Tutte polynomial. We shall use the phrase "*specialises to*" to indicate this. Thus for example, along $y = 0$, T specialises to the chromatic polynomial.

It turns out that the hyperbolae H_α defined by

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

play a special role in the theory. We note several important specialisations below.

(3.10) Along H_1, $T(G;x,y) = x^{|E|}(x-1)^{r(E)-|E|}$.

(3.11) Along H_2; when G is a graph T specialises to the partition function of the Ising model.

(3.12) Along H_Q, for general positive integer Q, T specialises to the partition function of the Potts model of statistical physics. These quantities are useful in simulations or computations of the probabilities of configurations of spins on the vertices of the graph.

(3.13) Along H_q, when q is a prime power, for a matroid M of vectors over $GF(q)$, T specialises to the weight enumerator of the linear code over $GF(q)$, determined by M.

(3.14) Along H_q for any positive, not necessarily integer, q, T specialises to the partition function of the random cluster model introduced by Fortuin and Kasteleyn [7].

(3.15) Along the hyperbola $xy = 1$ when G is planar, T specialises to the Jones polynomial of the alternating link or knot associated with G. This connection was first discovered by Thistlethwaite [18].

More details on these topics can be found in Welsh [20] and other more specialised interpretations can be found in the survey of Brylawski and Oxley [4].

4 The ferromagnetic random cluster model

As we mentioned above, as Q varies between $0 < Q < \infty$, T evaluates the partition function of the random cluster model. For integer Q this is the Q-state Potts model and when $Q = 2$ it is the Ising model. When $x \geq 1$ and $y \geq 1$, we have the region corresponding to *ferromagnetism*. In the case $Q = 2$ we know from Jerrum and Sinclair [11] that there is a fpras for all G. Here we obtain a similar result for general Q but only for the dense case.

For the remainder of this paper, except for Sections 8 and 10, we assume that we are dealing with the Tutte polynomial of an α-dense graph G.

A first easy, but essential, observation is the following. Let G_p denote the random graph obtained by selecting edges of G independently with probability p.

Lemma 1 *Assume G is connected with n vertices and m edges. Assume $x, y > 1$ and let $p = (y-1)/y$ and $Q = (x-1)(y-1)$. Let $\kappa = \kappa(G_p)$ be the number of components of G_p. Then*

$$T(G; x, y) = \frac{y^m}{(x-1)(y-1)^n} \mathbf{E}(Q^\kappa).$$

Proof

$$\begin{aligned} T(G; x, y) &= \sum_{A \subseteq E} (x-1)^{n-1-r(A)} (y-1)^{|A|-r(A)} \\ &= \sum_{A \subseteq E} (x-1)^{\kappa(A)-1} (y-1)^{|A|+\kappa(A)-n} \end{aligned}$$

where $\kappa(A)$ is the number of components of $G_A = (V, A)$. Thus

$$\begin{aligned} T(G; x, y) &= \frac{y^m}{(x-1)(y-1)^n} \sum_{A \subseteq E} \left(\frac{y-1}{y}\right)^{|A|} \left(\frac{1}{y}\right)^{m-|A|} ((x-1)(y-1))^{\kappa(A)} \\ &= \frac{y^m}{(x-1)(y-1)^n} \sum_{A \subseteq E} Q^{\kappa(A)} \mathbf{Pr}\{G_p = G_A\}. \end{aligned}$$

□

We now describe a property of dense graphs which is the key to much of the ensuing analysis.

Define $G^* = (V, E^*)$ by $(u, v) \in E^*$ if and only if $|N(u) \cap N(v)| \geq \alpha^2 n/2$.

Lemma 2 *G^* has at most $s = \lceil 2/\alpha \rceil - 1$ components.*

Proof Suppose that G^* has more than s components. Then there exist $v_1, v_2, \ldots v_{s+1}$ such that $|N(v_i) \cap N(v_j)| < \alpha^2 n/2$ if $i \neq j$. But then

$$\begin{aligned}
\left|\bigcup_{i=1}^{s+1} N(v_i)\right| &\geq \sum_{i=1}^{s+1} |N(v_i)| - \sum_{i \neq j} |N(v_i) \cap N(v_j)| \\
&> (s+1)\alpha n - \binom{s+1}{2}\frac{\alpha^2 n}{2} \\
&= (s+1)\alpha n\left(1 - \frac{s\alpha}{4}\right) \\
&\geq n.
\end{aligned}$$

□

Let $\hat{Q} = \max\{Q, Q^{-1}\}$ and $\zeta = y^m/((x-1)(y-1)^n)$.

We claim that the following algorithm estimates $T(G; x, y)$ for $G \in \mathcal{G}_\alpha$.

Algorithm EVAL

begin

  $p := \frac{y-1}{y}$; $Q := (x-1)(y-1)$;

  $t := \lceil 16\hat{Q}^{2s}\epsilon^{-2} \rceil$;

  for $i = 1$ **to** t **do**

  begin

    Generate G_p;

    $Z_i := Q^{\kappa(G_p)}$

  end

  $\tilde{Z} := \frac{Z_1 + Z_2 + \cdots + Z_t}{t}$;

  Output $Z = \zeta\tilde{Z}$

end

We first prove

Lemma 3 *In the notation of Lemma 1, let*

$$n_0 = \min\left\{n : n \geq \max\left\{\frac{32\ln(n\hat{Q})}{\alpha^3 p^2}, Q^{10/\alpha}\right\}\right\}.$$

If $n \geq n_0$ then

(a) $Q \geq 1$ implies

$$\mathbf{E}(Q^{2\kappa}) \leq 2Q^{2s}.$$

(b) $Q < 1$ implies

$$\mathbf{E}(Q^{\kappa}) \geq Q^s/2.$$

Proof Let the components of G^* be $C_1, C_2, \ldots C_\rho, \rho \leq s$. Let $\mathcal{E}_u$ denote the event $\{\kappa(G_p) > u\rho\}$ for $1 \leq u \leq u_0 = \lceil \alpha^2 n/8 \rceil$. If $\mathcal{E}_u$ occurs then at least one C_i must contain vertices from $u+1$ distinct components of G_p. In this case let $x_1, x_2, \ldots x_{u+1}$ be in the same component of G^* but in different components of G_p. The probability that G_p contains no path of length 2 connecting x_{2i-1} to x_{2i} for each i, $1 \leq i \leq \lfloor (u+1)/2 \rfloor$ is at most $(1-p^2)^K$, where $K = (\alpha^2 n/2 - 2u)u/2$. Hence

$$\begin{aligned} \mathbf{Pr}\{\mathcal{E}_u\} &\leq n^{u+1}(1-p^2)^K \\ &\leq (n^2 e^{-\alpha^2 p^2 n/8})^u, \qquad \text{for } u \leq u_0, n \geq n_0. \end{aligned}$$

Thus for $u \leq u_0, n \geq n_0$

$$\begin{aligned} \mathbf{Pr}\{\mathcal{E}_u\} &\leq (n^2 \exp\{-4\ln(n\hat{Q})/\alpha\})^u \\ &= (n^{2-4/\alpha}\hat{Q}^{-4/\alpha})^u. \end{aligned}$$

Suppose first that $Q \geq 1$. Then

$$\begin{aligned} \mathbf{E}(Q^{2\kappa}) &\leq Q^{2\rho}\left(1 + \sum_{u=1}^{u_0} Q^{2u\rho}\mathbf{Pr}\{\mathcal{E}_u\}\right) + Q^{2n}\mathbf{Pr}\{\mathcal{E}_{u_0}\} \\ &\leq Q^{2\rho}\left(1 + \sum_{u=1}^{u_0}(n^{2-4/\alpha}Q^{2\rho-4/\alpha})^u\right) + Q^{2n}n^{(2-4/\alpha)(\alpha^2 n/8)} \\ &\leq 2Q^{2\rho}, \end{aligned}$$

which deals with (a).

Suppose now that $Q < 1$. Then

$$\begin{aligned} \mathbf{E}(Q^{\kappa}) &\geq Q^{\rho}(1 - \mathbf{Pr}\{\mathcal{E}_1\}) \\ &\geq Q^{\rho}/2 \end{aligned}$$

for $n \geq n_0$, which deals with (b). □

Theorem 1 *For fixed rational x, y, and $\epsilon > 0$, if $T = T(G; x, y)$ and Z is the output of Algorithm EVAL, then*

$$\mathbf{Pr}\{|Z - T| \geq \epsilon T\} \leq \frac{1}{4}.$$

Proof Since $Z = \zeta\left(\frac{Z_1 + \ldots + Z_t}{t}\right)$, from Lemma 1 we see that $T = \mathbf{E}(Z)$. From Chebychev's inequality

$$\mathbf{Pr}\{|Z - T| \geq \epsilon T\} \leq \frac{\mathbf{Var}(Z)}{\epsilon^2 T^2} \leq \frac{\zeta^2}{\epsilon^2 t} \frac{\mathbf{Var}(Z_i)}{T^2} \leq \frac{\zeta^2}{\epsilon^2 t} \frac{\mathbf{E}(Z_i^2)}{T^2}.$$

Case $Q < 1$

Lemma 3 gives

$$\begin{aligned} \mathbf{E}(Z_i^2) &= \mathbf{E}(Q^{2\kappa(G_p)}) \leq 1 \\ T^2 &= \zeta^2(\mathbf{E}(Z_i))^2 = \zeta^2(\mathbf{E}(Q^{\kappa(G_p)}))^2 \\ &\geq \zeta^2 Q^{2s}/4 \end{aligned}$$

giving

$$\mathbf{Pr}\{|Z - T| \geq \epsilon T\} \leq \frac{4}{\epsilon^2 t Q^{2s}}.$$

Case $Q \geq 1$

$$\begin{aligned} \mathbf{Pr}\{|Z - T| \geq \epsilon T\} &\leq \frac{\zeta^2}{\epsilon^2 t} \frac{\mathbf{E}(Q^{2\kappa})}{T^2} \\ &\leq \frac{2Q^{2s}}{\epsilon^2 t} \end{aligned}$$

using Lemma 3, and noticing that for $Q \geq 1$, $T \geq \zeta$.

The result follows provided

$$t \geq \frac{16}{\epsilon^2 Q^{2s}} \quad (Q < 1)$$

and

$$t \geq \frac{8Q^{2s}}{\epsilon^2} \quad (Q \geq 1),$$

which it is by choice of t in EVAL. $\square$

Note: although polynomially bounded the running time grows when $(x-1)(y-1)$ or its inverse grow.

5 Reliability - $(x = 1, y \geq 1)$

The question here is: given a connected graph G and a rational p, $0 < p < 1$, can we efficiently estimate the *reliability probability*,

$$\phi(p) = \phi(G, p) = \mathbf{Pr}\{G_p \text{ is connected}\}.$$

This is well known to be a $\#P$-hard problem, but approximation algorithms for p very large and G planar, have been found by Karp and Luby [12]. Here we show that fully polynomial randomised approximation schemes exist for estimating reliability for the class of dense graphs for all values of p. Consider the following algorithm:

Algorithm RELIABILITY
begin
  $t := \lceil 4p^{-s}\epsilon^{-2} \rceil$;
  for $i = 1$ **to** t **do**
  begin
    Generate G_p;
    $Z_i = \begin{cases} 1 & G_p \text{ is connected} \\ 0 & G_p \text{ is not connected} \end{cases}$
  end
  $Z = \frac{Z_1 + Z_2 + \cdots + Z_t}{t}$;
  Output Z
end

Theorem 2 *The above algorithm is a fpras for estimating the reliability probability in the class of dense graphs.*

Proof We have to show that for n sufficiently large, the output Z satisfies

$$\mathbf{Pr}\{|Z - \phi(p)| \geq \epsilon\phi(p)\} \leq \frac{1}{4}.$$

Clearly $\mathbf{E}(Z) = \phi(p)$ and $\mathbf{Var}(Z) = \phi(p)(1 - \phi(p))/t$. Applying the Chebychev inequality

$$\mathbf{Pr}\{|Z - \phi(p)| \geq \epsilon\phi(p)\} \quad \leq \quad \frac{\mathbf{Var}(Z)}{\epsilon^2\phi(p)^2}$$

$$
\begin{aligned}
&\le \frac{1}{t\epsilon^2 \phi(p)} \\
&\le \frac{1}{4},
\end{aligned}
$$

provided

$$\phi(p) \ge p^s. \tag{1}$$

We now prove that (1) holds for n sufficiently large. As in the proof of Lemma 3 let G^* have components $C_1, C_2, \ldots, C_\rho$. Consider the multi-graph $\tilde{G}$ with vertices $\{1, 2, \ldots, \rho\}$ and an edge (i, j) for each edge of G joining C_i to C_j. In other words, $\tilde{G}$ is obtained from G by contracting each component C_i of G^* to a single vertex i. Since G is connected, $\tilde{G}$ contains a spanning tree. Let X be a fixed spanning tree of $\tilde{G}$.

Now G_p is connected if (i) $G_p \supseteq X$ and (ii) for each i and all $u, v \in C_i$ there exists w such that G_p contains the path u, w, v. Thus if A is the event (i) and B_i is the event (ii) then

$$
\begin{aligned}
\mathbf{Pr}(G_p \text{ is connected}) &\ge P(A \cap B_1 \cap \ldots \cap B_\rho) \\
&\ge P(A) \prod_{i=1}^{\rho} P(B_i)
\end{aligned}
$$

using the FKG inequality.

Clearly

$$P(A) = p^{\rho - 1}.$$

For fixed $u, v \in C_i$, the probability no (u, w, v) path exists is not more than

$$(1 - p^2)^{\alpha^2 n/2}.$$

Hence

$$P(B_i) \ge 1 - (1 - p^2)^{\alpha^2 n/2} \binom{|C_i|}{2}.$$

Thus

$$
\begin{aligned}
\phi(p) &\ge p^{\rho-1} \prod_{i=1}^{\rho} \left(1 - (1 - p^2)^{\alpha^2 n/2} \binom{|C_i|}{2}\right) \\
&\ge p^{\rho-1} \left(1 - (1 - p^2)^{\alpha^2 n/2} \sum_{i=1}^{\rho} \binom{|C_i|}{2}\right) \\
&\ge p^s \qquad \text{for}
\end{aligned}
$$

for n sufficiently large. $\square$

Note also that, for fixed p, the above algorithm works provided only that the network is not too sparse. Each vertex should have at least $\Omega(n/\ln n)$ neighbours.

6 Strong Connectivity - $(x = 0, y = 2)$

By dualising Stanley's result that $T(G;2,0)$ counts the acyclic orientations of G, we see that $T(G;0,2)$ enumerates the number of orientations of G which are *totally cyclic*, that is, every edge belongs to a directed cycle, see also [4]. Equivalently, an orientation of a connected graph G is totally cyclic if the resulting digraph is strongly connected.

Whereas we cannot see how to find a fpras for the number of acyclic orientations, even in dense graphs, we show that at (0,2) this is possible.

Here the question is: if we randomly orient the edges of G to form a digraph $\vec{G}$, can we estimate the probability $\psi(G)$ that $\vec{G}$ is strongly connected. We assume that G has no bridges, else $\psi(G) = 0$. We use the following algorithm.

Algorithm CONNECT
begin
  $t := \lceil \epsilon^{-2} 2^{2s+1} \rceil$
  for $i = 1$ **to** t **do**
  begin
    Generate $\vec{G}$;
    $Z_i = \begin{cases} 1 & \vec{G} \text{ is strongly connected} \\ 0 & \vec{G} \text{ is not strongly connected.} \end{cases}$
  end
  $Z = \frac{Z_1 + \cdots + Z_t}{t}$;
  Output Z
end

Clearly $\mathbf{E}(Z) = \psi(G)$ and $\mathbf{Var}(Z) = \psi(G)(1-\psi(G))/t$, so Chebychev's inequality gives

$$\begin{aligned} \mathbf{Pr}\{|Z - \psi(G)| \geq \epsilon\psi(G)\} &\leq \frac{1}{t\epsilon^2\psi} \\ &\leq 1/4 \end{aligned} \tag{2}$$

provided $t\epsilon^2\psi \geq 4$.

Lemma 4

$$\psi(G) \geq 2^{-(2s-1)},$$

for n sufficiently large.

Proof Consider the multi-graph $\tilde{G}$ defined in the proof of Theorem 2. It is bridgeless, as G is, and so it contains a spanning 2-edge connected subgraph Γ with at most $2\rho - 2$ edges. Thus by an old result of Robbins [16] there are at least two orientations of Γ which will make it strongly connected. Fix one such orientation w_0 and let $\mathcal{E}$ be the event that the random orientation is w_0. Then

$$\mathbf{Pr}\{\mathcal{E}\} \geq 2^{2-2\rho}.$$

Now $\vec{G}$ is strongly connected if (i) $\mathcal{E}$ occurs and (ii) for every component C_i of G^* and every $u, v \in C_i$ there are directed paths of length two from u to v which avoid the edges of Γ. For a fixed u, v, the probability of no such u, v path, given $\mathcal{E}$, is at most $(3/4)^{\alpha^2 n/2-2\rho}$ and so

$$\begin{aligned}
\psi(G) &\geq 2^{2-2\rho}\left(1 - n(n-1)\left(\frac{3}{4}\right)^{\alpha^2 n/2-2\rho}\right) \\
&\geq 2^{1-2s}
\end{aligned}$$

provided

$$n \geq \frac{2\ln(2n^2(4/3)^{2s})}{\alpha^2\ln(4/3)}.$$

□

Combining Lemma 4 with (2) gives:

Proposition 1 *The randomised algorithm CONNECT is a fpras for estimating the number of totally cyclic orientations of dense graphs.*

7 Other parts of the Tutte plane

The above arguments show that in the dense case T has a fpras in the region $x \geq 1$, $y > 1$. Annan [2] has dealt with the case $y = 1$, $x \geq 1$.

Now suppose that $x < 1$ and $y > 1$. Let $\tilde{x} = 2 - x$. Then

$$\begin{aligned} T(G;x,y) &= \sum_{A \subseteq E} (-1)^{n-1-r(A)} (\tilde{x}-1)^{n-1-r(A)} (y-1)^{|A|-r(A)} \\ &= \frac{y^m}{(\tilde{x}-1)(y-1)^n} \mathbf{E}((-1)^{\kappa-1} \tilde{Q}^{\kappa}) \end{aligned}$$

where $\kappa = \kappa(G_p)$ and $\tilde{Q} = (\tilde{x}-1)(y-1)$.

But

$$\begin{aligned} \mathbf{E}(((-1)^{\kappa-1}\tilde{Q}^{\kappa})^2) &= \mathbf{E}(\tilde{Q}^{2\kappa}) \\ &\leq 2\tilde{Q}^{2\rho}, \end{aligned}$$

where ρ is as in the proof of Lemma 3.

So if $|\mathbf{E}((-1)^{\kappa-1}\tilde{Q}^{\kappa})|$ is not too small then one can use Algorithm EVAL with a suitable value of t. Let $p_i = \mathbf{Pr}\{\kappa = i\}, i = 1, 2, \ldots, n$. Since p_i is negligible for $i > \rho$ we can deduce that unless $\tilde{Q}$ is close to a root of

$$\sum_{i=1}^{\rho} (-1)^i p_i z^i = 0, \qquad (3)$$

then $|\mathbf{E}((-1)^{\kappa-1}\tilde{Q}^{\kappa})|$ will be sufficiently large and we will be able to approximate T.

If $\alpha > 1/2$ then G_p is connected with high probability since every pair of vertices have at least $(2\alpha - 1)n$ common neighbours. We can then take $\rho = 1$ in (3) and there is no problem.

The approach does not seem to yield anything useful for $x > 1$ and $y < 1$. Putting $\tilde{y} = 2 - y$ introduces a factor $(-1)^{|A|-r(A)}$ into the sum which is not easy to deal with.

8 Random Graphs

Apart from its intrinsic interest, some insight into the limitations of the above methods is gained by considering the case of an input which is a random graph.

First fix x, y both strictly greater than 1, as the point at which we aim to approximate T. Now suppose that we apply Algorithm EVAL to an input G, chosen randomly from $\mathcal{G}_{n,p_1}$; with the slight modification that we allow EVAL to run for a time

$$\tau = \lceil 16\hat{Q}^2\epsilon^{-2} \rceil$$

where as usual $Q=(x-1)(y-1)$ and $\hat{Q}=\max\{Q,Q^{-1}\}$.

Call this modified version EVAL$'$.

Lemma 5 *Let Z be the random output of EVAL$'$. If $T=T(G_{n,p_1};x,y)$ then provided*

$$p_1 \geq 8\left(\frac{\ln n}{n}\right)\left(\frac{y}{y-1}\right)$$

$$\lim_{n\to\infty}\mathbf{Pr}_{p_1}\left(\mathbf{Pr}\{|Z-T|\geq \epsilon T\}\leq \frac{1}{4}\right)=1.$$

Our notation is that $\mathbf{Pr}_{p_1}$ denotes probabilities computed over the space of random graphs G_{n,p_1}. $\mathbf{Pr}_p$ denotes (conditional) probabilities computed over the space of subgraphs of G_{n,p_1}. $\mathbf{Pr}_{p_2}$ denotes probabilities computed over G_{n,p_2}, where $p_2=pp_1$.

Proof Recall how EVAL works. On input G and p it successively generates, independently, G_p and then outputs

$$Z=\zeta\left(\frac{Z_1+\ldots+Z_t}{t}\right),$$

where $Z_i=Q^{\kappa(G_p)}$ and $p=(y-1)/y$. Here G is random from $\mathcal{G}(n,p_1)$ so G_p can be regarded as drawn randomly from $\mathcal{G}(n,p_2)$.

Examining now the proof of Theorem 1, we see that what we need to do is bound $\mathbf{E}_{p_2}(Z^2)$.

In the following estimate $k_1,k_2,\ldots,k_t$ are the sizes of components with at most $n/2$ vertices.

$$\begin{aligned}
\mathbf{E}_{p_1}(\mathbf{Pr}_p(\kappa(G_p)=t+1)) &= \mathbf{Pr}_{p_2}\{\kappa(G_p)=t+1\}\\
&\leq \sum_{\substack{k_1+k_2+\cdots+k_t\leq n\\ 1\leq k_i\leq n/2}}\prod_{i=1}^{t}\binom{n}{k_i}(1-p_2)^{k_i(n-k_i)/2}\\
&\leq \sum_{\substack{k_1+k_2+\cdots+k_t\leq n\\ 1\leq k_i\leq n/2}}\prod_{i=1}^{t}\left(\frac{ne}{k_i}e^{-np_2/2}\right)^{k_i/2}\\
&\leq \sum_{\substack{k_1+k_2+\cdots+k_t\leq n\\ 1\leq k_i\leq n/2}}\prod_{i=1}^{t}(en^{-3})^{k_i/2}\\
&= \sum_{\substack{k_1+k_2+\cdots+k_t\leq n\\ 1\leq k_i\leq n/2}}(en^{-3})^{(k_1+k_2+\cdots+k_t)/2}
\end{aligned}$$

$$
\begin{aligned}
&\le \sum_{k=t}^{n} \binom{k-1}{t-1} (en^{-3})^{k/2} \\
&= (1+o(1))(en^{-3})^{t/2}.
\end{aligned}
$$

So

$$\mathbf{Pr}_{p_1}(\mathbf{Pr}_p(\kappa(G_p) = t+1) \ge n^{-t}) \le (en^{-1/2})^t$$

and

$$\mathbf{Pr}_{p_1}(\exists t : 1 \le t < n : \mathbf{Pr}_p(\kappa(G_p) = t+1) \ge n^{-t}) = O(n^{-1/2}).$$

We can assume therefore that $G = G_{n,p_1}$ satisfies

$$\mathbf{Pr}_p(\kappa(G_p) = t+1) \le n^{-t}. \tag{4}$$

We can now proceed as we did for dense graphs.

Case: $Q < 1$:

$$
\begin{aligned}
\mathbf{E}_p(Q^\kappa) &\ge Q\mathbf{Pr}_p(\kappa(G_p) = 1) \\
&\ge Q\left(1 - \frac{1}{n} - \frac{1}{n^2} - \cdots\right) \\
&\ge Q/2 \qquad\qquad \text{for } n \ge 2,
\end{aligned}
$$

and so

$$
\begin{aligned}
\mathbf{E}_p(Z) &\ge \zeta Q/2 \\
\mathbf{Var}_p(Z) &\le \zeta^2/\tau
\end{aligned}
$$

and

$$
\begin{aligned}
\mathbf{Pr}_p(|Z - \mathbf{E}_p(Z)| \ge \epsilon \mathbf{E}_p(Z)) &\le \frac{4\zeta^2}{\epsilon^2\zeta^2\tau Q^2} \\
&\le \frac{1}{4}.
\end{aligned}
$$

Case: $Q \ge 1$: if

$$t_0 = \left\lceil \frac{10n \ln Q}{\ln n} \right\rceil,$$

then

$$\begin{aligned}\mathbf{E}_{p_1}\mathbf{E}_p(Z_i^2) &\leq Q^2 + \sum_{t=2}^{t_0} \frac{Q^{2t}}{n^{t-1}} + Q^{2n-3n} \\ &\leq 2Q^2\end{aligned}$$

and so

$$\begin{aligned}\mathbf{E}_p(Z) &\geq \zeta \\ \mathbf{Var}_p(Z) &\leq 2\zeta^2 Q^2/\tau\end{aligned}$$

and

$$\begin{aligned}\mathbf{Pr}_p(|Z - \mathbf{E}_p(Z)| \geq \epsilon \mathbf{E}_p(Z)) &\leq \frac{2\zeta^2 Q^2}{\epsilon^2 \zeta^2 \tau} \\ &\leq \frac{1}{4}.\end{aligned}$$

□

What we would really like is to be able to choose G_{n,p_1} first and then x, y arbitrarily, instead of considering them fixed.

Note also that we can effectively deal with points $x < 1, y > 1$ as in Section 7, since (4) implies $|\mathbf{E}((-1)^{\kappa-1}\tilde{Q}^{\kappa})| \approx \tilde{Q}$.

9 Is exact counting hard?

The proof in [9] that evaluating T is $\#P$-hard, at all but a few points, does not show it is hard in the case of dense graphs. We do not propose to classify which parts of the plane are $\#P$-hard in the dense case, however the following results suggest that there is considerable variation in behaviour, so that a complete characterisation may be difficult.

Lemma 6 *Even when G is dense, evaluating $T(G; a, 1)$ for $a \neq 1$, cannot be done in polynomial time unless $NP = RP$.*

Proof The *k-thickening* of a graph G is the graph obtained by replacing each edge $\{u, v\}$ by k parallel edges with endpoints u, v. From [9] we know that the k-thickening G^k of G has Tutte polynomial given by

$$T(G^k;x,y) = (1+y+\ldots+y^{k-1})^{n-r(G)}T(G;X,Y)$$

where

$$\begin{aligned} X &= \frac{x+y+\ldots+y^{k-1}}{1+y+\ldots+y^{k-1}} \\ Y &= y^k. \end{aligned}$$

Suppose that there exists a polynomial time algorithm evaluating T for dense graphs at $(a,1)$. Then for any dense G we can find a succession of thickenings $G^2, G^3, \ldots$ which are also dense and

$$T(G^k;a,1) \approx T(G;z_k,1)$$

where $\approx$ is interpreted as equality up to multiplication by an easily determined constant and

$$z_k = (a+k-1)/k.$$

Provided $a \neq 1$ this gives us enough points to recover $T(G;2,1)$ by Lagrange interpolation. But Annan [2] has shown that even in the dense case, $T(G;2,1)$ (equalling the number of forests of G) has no polynomial-time evaluation algorithm unless $NP = RP$. □

Similarly, let $(a,b) \in$ hyperbola H_λ with λ a positive integer. Then we can write

$$\begin{aligned} T(G;a,b) &= \sum_A (a-1)^{r(E)-r(A)}(b-1)^{|A|-r(A)} \\ &= (a-1)^{r(E)} \sum_A \lambda^{|A|-r(A)}(a-1)^{-|A|}. \end{aligned}$$

Suppose we can evaluate T for $G \in \mathcal{G}_\alpha$ at (a,b). Then consider the transformation $G \mapsto G^k$;

$$T(G^k;x,y) \approx T(G;X,Y)$$

where X and Y are as given above.

Take $x=a$, $y=b$, and since $G \to G^k$ preserves density, we obtain evaluations of $T(G)$ at enough points along the hyperbola H_λ to be able to interpolate $T(G;1-\lambda,0)$. But this gives the number of λ-colourings of G and from Edwards [6] we know that if $\alpha < \frac{\lambda-2}{\lambda-1}$ this evaluation is $\#P$-hard for $\lambda \geq 3$. Hence we have:

for $(a,b) \in H_\lambda$, λ integer ≥ 3 and α satisfying $0 < \alpha < \frac{\lambda-2}{\lambda-1}$ it is $\#P$-hard to evaluate $T(G;a,b)$ for $G \in \mathcal{G}_\alpha$.

This illustrates the point that a complete characterisation of the difficulty of exact evaluation in the dense case may prove difficult. For example, the main result of Edwards [6] is that for $\alpha > (\lambda-2)/(\lambda-1)$, exact evaluation of the number of λ-colourings is in P. In other words:

evaluating $T(G;1-\lambda,0)$ is in P whenever $G \in \mathcal{G}_\alpha$ and $\alpha > (\lambda-2)/(\lambda-1)$.

This critical cut off, in which there exists some α_c (in this case $\alpha_c = (\lambda-2)/(\lambda-1)$) which separates tractable from almost certainly intractable, may well extend to randomised approximation. This is because Edwards also showed it was NP-hard to decide if G had a λ-colouring when $\alpha < (\lambda-3)/(\lambda-2)$ but was in P for larger values of α. Thus, an immediate consequence is:

Corollary 1 *Even in the case of dense $G \in \mathcal{G}_\alpha$, if $\alpha < (\lambda-3)/(\lambda-2)$, where λ is a positive integer, there is no fpras for estimating T at $(1-\lambda,0)$ unless $NP = RP$.*

It is interesting that in the region

$$\left(\frac{\lambda-3}{\lambda-2}\right) < \alpha < \left(\frac{\lambda-2}{\lambda-1}\right),$$

where the decision problem is easy but exact counting is hard, there is no obvious obstacle to the existence of a fpras.

10 Extension to Linear Matroids

The above results can be extended to a class of *dense linear* matroids in a fairly natural way. Let M be an $m \times n$ matrix over some field F. Let $\bar{M}$ be the $m \times n$ 0-1 matrix with $\bar{M}_{i,j} = 1$ if and only if $M_{i,j} \neq 0$. Then let $\rho_i = \rho_i(M) = \sum_{j=1}^{n} \bar{M}_{i,j}$.

For $0 < \alpha < 1$ and $k \geq 3$ let

$\mathcal{M}_{\alpha,k} = \{M$: (i) $\rho_i \geq \alpha\binom{m}{k-1}$, (ii) each column of $\bar{M}$ has at most k 1's and (iii) the columns of $\bar{M}$ are distinct.$\}$

Assume w.l.o.g. that M has full row rank. Then the Tutte polynomial $T(M;x,y)$ can be expressed as follows

$$T(M;x,y) = \sum_{A\subseteq[n]} (x-1)^{m-r(A)}(y-1)^{|A|-r(A)}$$

where $r(A)$ is the rank of the sub-matrix of M induced by the columns $M_j, j \in A$

$$= \frac{y^n}{(y-1)^m} \sum_{A\subseteq[n]} Q^{m-r(A)} p^{|A|}(1-p)^{n-|A|},$$

where $Q = (x-1)(y-1)$ and $p = (y-1)/y$ as before,

$$= \frac{y^n}{(y-1)^m} \mathbf{E}(Q^{m-r}), \tag{5}$$

where $r = r(M_p)$ and M_p is the random sub-matrix of M obtained by including each column with probability p. We are assuming here that $x, y > 1$.

We first prove a lemma serving the same purpose as Lemma 2.

Lemma 7 *If $A \in \mathcal{M}_{\beta,k}$ then*

$$r(A) \geq m - (2k \ln m)/\beta,$$

provided $m \geq 3k$.

Proof We will prove the existence of an $h \times h$ permutation matrix H, $h \geq m - (2k\ln m)/\beta$, which is a submatrix $\bar{A}$. This will clearly prove the lemma.

Put $s = \lceil 2\ln m/\beta \rceil$ and let $S_1, \ldots, S_s$ be s random subsets of the rows of $\bar{A}$, where each subset S_i is chosen randomly and independently according to a uniform distribution among all subsets of cardinality at most $k-1$ of $[m]$. For each i, $1 \leq i \leq m$, let A_i denote the *complement* of the following event; row i is in at least one of the sets S_j or there is a subset S_j so that $\{i\} \cup S_j$ is precisely the set of ones of a column of $\bar{A}$. We claim that the probability of each event A_i is at most $(1-\beta/2)^s < 1/m$. To see this, observe that if i is not in any of the sets S_j, then these sets are random subsets of cardinality at most $k-1$ of $[m] - \{i\}$. By assumption there are at least $\beta\binom{m}{k-1}$ distinct columns of $\bar{A}$ which have a 1 in row number i. The conditional probability that for a fixed j, S_j is not the set of ones of such a column without i, given that S_j does not contain i, is at most

$$1 - \frac{\beta\binom{m}{k-1}}{\sum_{l=0}^{k-1}\binom{m-1}{l}} \leq 1 - \frac{\beta}{2},$$

where here we applied the fact that $m \geq 3k$. Since the subsets S_j are chosen independently the probability of each A_i is indeed at most $(1-\beta/2)^s < 1/m$, as claimed.

It follows that with positive probability none of the events A_i occurs. Let $S_1, \ldots, S_s$ be a fixed choice for the sets S_j for which no event A_i occurs. Define $T = [m] - \cup_{j=1}^s S_j$. Observe that for each row i in T there is a column c_i of $\bar{A}$ that has a one in row i and in no other row of T. The submatrix of $\bar{A}$ on the rows in T and the columns $c_i, i \in T$ is a permutation matrix, as required. Since $|T| \geq m - s(k-1) \geq m - 2k \ln m/\beta$ the desired result follows. $\square$

We can modify Algorithm EVAL of Section 4 to estimate $\mathbf{E}(Q^{m-r})$ by putting

$$t = \lceil 16 m^d \epsilon^{-2} \rceil,\ d = 8k \ln \hat{Q}/(\alpha p),\ Z_i = Q^{m-r} \text{ and } \zeta = y^n/(y-1)^m.$$

The validity of this approach depends on the following lemma, where we assume that $k \geq 3$ since the case $k = 2$ (corresponding to graphs) had already been considered.

Lemma 8 *If $k \geq 3$ and $m \geq m_1(Q, k, \alpha, p)$ then*

(a) $Q \geq 1$ *implies* $\mathbf{E}(Q^{2(m-r)}) \leq 2m^d$,

(b) $Q \leq 1$ *implies* $\mathbf{E}(Q^{m-r}) \geq \frac{1}{2} m^{-d/2}$.

Proof Let $\mathcal{E}$ denote the event $\{\bar{M}_p \notin \mathcal{M}_{\alpha p/2}\}$. Applying the Chernoff bound for the tails of the binomial distribution (see, for example, Alon and Spencer [1])

$$\Pr(\mathcal{E}) \leq m \exp\left\{-\alpha \binom{m}{k-1} p/8\right\}.$$

Applying Lemma 7 we see that if $Q \geq 1$,

$$\begin{aligned} \mathbf{E}(Q^{2(m-r)}) &\leq Q^{(8k \ln m)/(\alpha p)} + Q^m \Pr(\mathcal{E}) \\ &\leq 2m^d, \end{aligned}$$

and if $Q \leq 1$,

$$\begin{aligned} \mathbf{E}(Q^{m-r}) &\geq Q^{(4k \ln m)/(\alpha p)}(1 - \Pr(\mathcal{E})) \\ &\geq \frac{1}{2} m^{-d/2}. \end{aligned}$$

$\square$

11 Conclusion

(a) For $x \geq 1$, $y \geq 1$ there exists a fpras for all dense graphs; it is open whether one exists for non dense graphs.

(b) For $x < 1$, $y > 1$, there exists a fpras for *strongly dense* graphs ($\alpha > \frac{1}{2}$); again the question is open in the remaining case.

At a few special points of this region, namely $(x = (2^k - 2)/(2^k - 1), y = 2^k)$ $(k = 1, 2, ...)$ there is a fpras for all dense graphs [via the k-thickening at (0,2)].

It would be very surprising if these were just sporadic *good points.*

(c) For $x > 0$, $y < 1$, the situation is completely open. A key point here is $(2, 0)$ which enumerates acyclic orientations.

A possibly easier subregion is $x \geq 1$, $y < -1$, but the obvious map $(x, y) \mapsto (x, -y)$ doesn't seem to work.

(d) For $x < 0$, $y \leq 1$, the antiferromagnetic region, the situation is more variable and more interesting.

For example the arguments of Jerrum and Sinclair [11] and Welsh [22] show that unless $NP = RP$, there is no fpras along the curves where the hyperbolae $(x - 1)(y - 1) = Q$ for integer $Q \geq 2$, intersect this region.

One possible scenario is that the following is true:

For each (x, y) either exact evaluation is in P or there exists a critical density $\alpha_c(x, y)$, which separates the tractable case from the intractable, where intractable is to be interpreted in the sense "No fpras exists unless some very unlikely complexity hypothesis (such as $NP = RP$) is true".

If this is the case, then in the region $x \geq 1$, $y \geq 1$, $\alpha_c(x, y) = 0$, by our earlier argument. However it still seems more plausible that, as conjectured in [17], there exists an fpras throughout this region, regardless of density.

Acknowledgement

The original impetus to look at evaluations of T in the dense case, arose in discussions with Marek Karpinski in a RAND meeting in Oxford in September 1992. Further discussions with Joel Spencer, Nabil Kahale and James Annan have also been very helpful.

References

[1] Alon, N. and Spencer, J. H. *The Probabilistic Method*, John Wiley and Sons (1991).

[2] Annan, J.D. A randomised approximation algorithm for counting the number of forests in dense graphs, *Combinatorics, Probability and Computing,* (to appear).

[3] Broder, A. Z. , How hard is it to marry at random? (On the approximation of the permanent), proceedings of the 18th Annual ACM Symposium on Theory of Computing, (1986), 50-58.

[4] Brylawski, T.H. and Oxley, J.G. The Tutte polynomial and its applications, *Matroid Applictions* (ed. N. White), Cambridge Univ. Press, (1992), 123-225.

[5] Dyer M.E., Frieze A.M. and Jerrum M.R., Approximately counting Hamilton cycles in dense graphs, *Proceedings of the 4th Annual Symposium on Discrete Algorithms* (1994), 336-343.

[6] Edwards, K. The complexity of colouring problems on dense graphs, *Theoretical Computer Science* 43, (1986), 337-343.

[7] Fortuin, C.M. and Kasteleyn, P.W., On the random cluster model I. Introduction and relation to other models, *Physica*, 57, (1972), 536-564.

[8] Garey, M.R. and Johnson, D.S. *Computers and Intractability - A guide to the theory of NP-completeness.*, San Francisco, Freeman, (1979).

[9] Jaeger, F., Vertigan, D.L., Welsh, D.J.A. On the computational complexity of the Jones and Tutte polynomials, *Math. Proc. Camb. Phil. Soc.*, 108, (1990), 35-53.

[10] Jerrum, M. R. and Sinclair, A. A Monte-Carlo Algorithm for Estimating the Permanent, *SIAM Journal on Computing* 22 (1993), pp.284-293.

[11] Jerrum, M.R. and Sinclair, A. Polynomial-time approximation algorithms for the Ising model, *Proc. 17th ICALP, EATCS,* (1990), 462-475.

[12] Karp, R.M. and Luby, M. Monte-Carlo algorithms for the planar multiterminal network reliability problem, *Journal of Complexity*, 1, (1985), 45-64.

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

[14] Oxley, J.G. and Welsh, D.J.A. The Tutte polynomial and percolation, *Graph Theory and Related Topics* (eds. J.A. Bondy and U.S.R. Murty), Academic Press, London, (1979), 329-339.

[15] Rosenstiehl, P. and Read, R.C. On the principal edge tripartition of a graph, *Ann. Discrete Math.* 3, (1978), 195-226.

[16] Robbins, H.E. A theorem on graphs, with an application to a problem in traffic control, *Amer. Math. Monthly*, 46, (1939), 281-283.

[17] Stanley, R.P. Acyclic orientations of graphs, *Discrete Math*, **5**, (1973), 171-178.

[18] Thistlethwaite, M.B. A spanning tree expansion of the Jones polynomial, *Topology*, 26, (1987), 297-309.

[19] Vertigan, D.L. and Welsh, D.J.A. The computational complexity of the Tutte plane: the bipartite case. *Combinatorics, Probability and Computing*, 1, (1992), 181-187.

[20] Welsh, D.J.A. *Complexity: Knots, Colourings and Counting*, London Mathematical Society Lecture Note Series 186, Cambridge University Press, (1993).

[21] Welsh D.J.A. Randomised approximation schemes for Tutte-Grothendieck invariants, *Proc. IMA Workshop on Probability and Algorithms*, Minneapolis, September (1993).

[22] Welsh, D.J.A. Randomised approximation in the Tutte plane, *Combinatorics, Probability and Computing*, (to be published).

[23] Zaslavsky, T. Facing up to arrangements: face count formulas for partitions of spaces by hyperplanes, *Memoirs of American Mathematical Society* 154, (1975).