The Tutte Polynomial Modulo a Prime

A.J. Goodall [1]

Mathematical Institute, 24-29 St Giles', Oxford OX1 3LB, United Kingdom

Abstract

For F_p the field on prime number $p > 3$ elements, it has been conjectured that there are just $p+3$ evaluations of the Tutte polynomial in F_p which are computable in polynomial time. In this note it is shown that if $p \not\equiv -1 \bmod 12$ then there are further polynomial-time computable evaluations.

1 Definitions and introduction

Let $G = (V, E)$ denote a graph, with loops and parallel edges permitted, and $\mathcal{G}$ the collection of all such graphs. The *size* of a graph $G = (V, E)$ is $|E|$. If G has $k(G)$ connected components, then the *rank* of G, denoted $r(E)$, is $|V| - k(G)$. The rank $r(A)$ of a subset of edges $A \subseteq E$ is the rank of the subgraph (V, A).

Let X, Y be commuting indeterminates. The Tutte polynomial $T(G; X, Y)$ is a map $T : \mathcal{G} \to \mathbb{Z}[X, Y]$ defined for all graphs G by

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

An *evaluation* of the Tutte polynomial in a commutative ring R with 1 is a map $T(x, y) : \mathcal{G} \to \mathbb{Z}[x, y] \subseteq R$ obtained from T by substituting $(x, y) \in R \times R$ for the indeterminate pair (X, Y) in (1).

For all commutative rings R with unity 1 and $(x, y) \in R \times R$,

$$(x-1)(y-1) = 1 \quad \Rightarrow \quad T(G; x, y) = x^{|E|}(x-1)^{r(E)-|E|}. \tag{2}$$

[1] Partially supported by EPSRC

A theorem of [3] determines *all* the evaluations of the Tutte polynomial in $\mathbb{C}$ which are polynomial-time computable in the size of the graph G. Apart from those covered by (2) they are at the points

$$(-1,0),(0,-1),(1,1),(-1,-1), \tag{3}$$

and

$$(i,-i),(-i,i),(j,j^2),(j^2,j), \tag{4}$$

where $i=\sqrt{-1}$ and $j=(-1+\sqrt{-3})/2$.

In [7, §7.5] it is shown that all evaluations of the Tutte polynomial in F_2 are polynomial-time computable. All four evaluations in F_2 reduce to finding the parity of evaluations in $\mathbb{Z}$ at points in (2) and (3).

Annan [1] proved the following result.

Theorem 1 [1, §3.6] *Provided random polynomial time $\mathcal{RP}$ is not equal to $\mathcal{NP}$, the only polynomial-time computable evaluations of the Tutte polynomial in F_3 are at the points $(-1,0),(0,-1),(1,1),(-1,-1)$ and $(0,0)$.* □

He conjectured that similarly, for any prime $p>3$, the only polynomial-time computable evaluations of the Tutte polynomial in F_p correspond to the points covered by (2) and the points $(-1,0),(0,-1),(1,1),(-1,-1)$ in $F_p\times F_p$ corresponding to the points (3) in $\mathbb{C}\times\mathbb{C}$.

However, it will be shown that this conjecture needs to be modified to include further pairs of points corresponding to (4) when -1 or -3 is a square in F_p.

2 Polynomial-time evaluations of the Tutte polynomial in F_p

Call a point $(x,y)\in R\times R$ *easy* if the evaluation $T(G;x,y)$ in R is polynomial-time computable in the size of G.

For a ring homomorphism π note that $\pi(T(G;x,y))=T(G;\pi(x),\pi(y))$. The easy points (3) in $\mathbb{Z}\times\mathbb{Z}$ and the homomorphism $\pi:\mathbb{Z}\to R$, $z\mapsto z1$, ensure that $(-1,0),(0,-1),(1,1),(-1,-1)$ are easy in any commutative ring R with unity 1. This observation is made in [1, §3.6] for $R=F_p$.

The following shows that the points of (4) yield further easy points in F_p for $p\equiv 1 \bmod 4$ or $p\equiv 1 \bmod 3$. The *Legendre symbol* (a/p) is defined to be $+1$ when a is a non-zero square in F_p and -1 when a is not a square.

Theorem 2 *Let $p > 3$ be a prime. There are (at least) $p+5+(-1/p)+(-3/p)$ polynomial-time computable evaluations of the Tutte polynomial in F_p. These are at the following points in $F_p \times F_p$:*

$$\{(x, y) \in F_p \times F_p : (x-1)(y-1) = 1\}; \tag{5}$$

$$(-1, 0), (0, -1), (1, 1), (-1, -1); \tag{6}$$

$$(a, -a), (-a, a), \tag{7}$$

if $p \equiv 1 \bmod 4$ and $a^2 + 1 = 0$ in F_p; and,

$$(b, b^2), (b^2, b), \tag{8}$$

if $p \equiv 1 \bmod 3$ and $b^2 + b + 1 = 0$ in F_p.

PROOF. For each odd prime $p \in \mathbb{N}$ there are ideals of norm p in $\mathbb{Z}[i]$ if and only if $(-1/p) = +1$, or $p \equiv 1 \bmod 4$, and in $\mathbb{Z}[j]$ if and only if $(-3/p) = +1$, or $p \equiv 1 \bmod 3$.

Hence, for $p \equiv 1 \bmod 4$, there is a prime $r + si \in \mathbb{Z}[i]$ with norm $r^2 + s^2 = p$ and the homomorphism $\pi : \mathbb{Z}[i] \to \mathbb{Z}[i]/(r + si)$ gives images of the easy points $(i, -i), (-i, i) \in \mathbb{Z}[i]$ in the quotient ring. The homomorphic images of the points $(i, -i), (-i, i)$ do not coincide with the points given by (5) since $(i-1)(-i-1) = 2$, nor with the points $(1, 1), (-1, -1)$ of (6), since $p > 2$, nor with $(-1, 0), (0, -1)$ since $\pm i$ are units and cannot be mapped to 0.
The ideal $(r+si)$ is prime in the ring of ideals of $\mathbb{Z}[i]$, so the quotient $\mathbb{Z}[i]/(r+si)$ is a field, has p elements, and hence is isomorphic to F_p.

Similarly, for $p \equiv 1 \bmod 3$, there is prime $r+sj \in \mathbb{Z}[j]$ with norm $r^2-rs+s^2 = p$ and the homomorphism $\pi : \mathbb{Z}[j] \to \mathbb{Z}[j]/(r + sj)$ onto a field isomorphic to F_p has in its domain the easy points $(j, j^2), (j^2, j) \in \mathbb{Z}[j]$. The homomorphic images of these two points cannot coincide with any points in (5), (6), (7) since $(j-1)(j^2-1) = 3$ and $p > 3$. $\square$

When $p \in \mathbb{Z}$ does not split in the larger ring $\mathbb{Z}[i]$ or $\mathbb{Z}[j]$ it generates a prime ideal (p) of norm p^2. The quotient ring is then isomorphic with F_{p^2}. The proof of Theorem 2 gives the following.

Corollary 3 *For odd prime $p \equiv -1 \bmod 4$ or $p \equiv -1 \bmod 3$, the points listed in (2), (3), (4) provide $p^2 + 5 - (-1/p) - (-3/p)$ easy points in $F_{p^2} \times F_{p^2}$ via the homomorphism(s) $\mathbb{Z}[i] \to \mathbb{Z}[i]/(p)$ and/or $\mathbb{Z}[j] \to \mathbb{Z}[j]/(p)$.* $\square$

For $p \equiv 1 \bmod 12$, p^2+7 easy points in $F_{p^2} \times F_{p^2}$ arise from (2) and evaluation in the subfield isomorphic to F_p: all 8 points in (6), (7), (8) exist for this p. It is a small step to deduce the following.

Corollary 4 *Let $p > 3$ be prime and $n \geq 1$. If n is odd then there are $p^n + 5 + (-1/p) + (-3/p)$ polynomial-time computable evaluations of the Tutte polynomial in F_{p^n}. If n is even then there are p^n+7 polynomial-time computable evaluations of the Tutte polynomial in F_{p^n}.*

PROOF. In $F_{p^n} \times F_{p^n}$ there are $p^n - 1$ points satisfying (2). Further easy points correspond to the $6 + (-1/p) + (-3/p)$ points (6), (7), (8) of Theorem 2, evaluation being in the subfield F_p of F_{p^n}. For n even, Corollary 3 provides polynomial-time evaluations in the subfield F_{p^2} for the $2 - (-1/p) - (-3/p)$ remaining points. $\square$

There are $2^n + 2$ easy evaluations in F_{2^n} for $n \geq 1$. There are no elements of multiplicative order 4, and for even n, when there are two elements b, b^2 of order 3, the points $(b, b^2), (b^2, b)$ are such that $(b-1)(b^2-1) = 3 = 1$ in F_{2^n} and so are counted already under (2).

There are $3^n + 3 + (-1)^n$ easy evaluations in F_{3^n} for $n \geq 1$, with no elements order 3 and, for even n, two elements order 4. The point $(-1, -1)$ is already counted under (2) since $(-1-1)(-1-1) = 4 = 1$ in F_{3^n}.

Interpreting evaluation in F_p as "counting modulo p" it is natural to extend Theorem 2 from evaluation in $\mathbb{Z}/p\mathbb{Z}$ to evaluation in $\mathbb{Z}/m\mathbb{Z}$ for composite m by use of the Chinese Remainder Theorem. For prime $p > 3$ there are $1 + (-1/p)$ elements of multiplicative order 4 in $\mathbb{Z}/p^n\mathbb{Z}$ and $1 + (-3/p)$ elements of order 3. In $\mathbb{Z}/2^n\mathbb{Z}$, -1 is a square only if $n = 1$ and -3 is a square only if $n = 1, 2$. In $\mathbb{Z}/3^n\mathbb{Z}$, -1 is not a square and -3 is only a square for $n = 1$. By counting the number of solutions to $a^2 \equiv -1 \bmod m$ and $(2b+1)^2 \equiv -3 \bmod m$ the following is obtained.

Corollary 5 *Let $3 < m \in \mathbb{N}$ have $s \geq 0$ distinct prime factors greater than 3 and let $\phi(m)$ denote Euler's totient function. Denote by $e(m)$ the number of polynomial-time computable evaluations of the Tutte polynomial in $\mathbb{Z}/m\mathbb{Z}$. Then Theorem 2 yields the following lower bounds on $e(m)$, the number of easy points in $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.*

If $m \not\equiv 0 \bmod 4$ and each of the odd prime factors $p > 2$ of m satisfy $p \equiv 1 \bmod 12$, then

$$e(m) \geq \phi(m) + 4 + 2^{s+1}. \tag{9}$$

If $m \not\equiv 0 \bmod 4$ *and each of the odd prime factors* $p > 2$ *of* m *satisfy* $p \equiv 1 \bmod 4$*, at least one of which satisfies* $p \equiv 5 \bmod 12$*,*

or *if* $m \not\equiv 0 \bmod 8$*,* $m \not\equiv 0 \bmod 9$ *and there are* $s \geq 1$ *distinct prime factors* $p > 3$ *of* m *each satisfying* $p \equiv 1 \bmod 3$*, at least one of which satisfies* $p \equiv 7 \bmod 12$ *if* $m \not\equiv 0 \bmod 4$ *and* $m \not\equiv 0 \bmod 3$*, then*

$$e(m) \geq \phi(m) + 4 + 2^s. \tag{10}$$

Otherwise,

$$e(m) \geq \phi(m) + 4. \tag{11}$$

□

Whether these inequalities for $e(m)$ can be improved to equalities depends on whether Theorem 2 describes *all* the easy points in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. This question is briefly discussed in the following section.

3 Conclusion

For primes $p > 3$ it remains an open problem to determine if all the polynomial-time computable evaluations of the Tutte polynomial in F_p have been found. A revised version of the conjecture made in [1, §3.6] is the following.

Conjecture 6 *Let* $p > 3$ *be prime. Provided* $\mathcal{RP} \neq \mathcal{NP}$*, any evaluation of the Tutte polynomial in* F_p *not listed in Theorem 2 is not computable by a randomised polynomial-time algorithm.*

In [1, §3.7] some partial confirmation for this conjecture is adduced. Annan shows that evaluating the Tutte polynomial at the following points cannot be random polynomial time unless $\mathcal{RP} = \mathcal{NP}$:

$$\{(1, y) \in F_p \times F_p : y \neq 1\}, \tag{12}$$

and,

$$\{(x, y) \in F_p \times F_p : (x-1)(y-1) \neq 0, 1, 2;\ \langle x \rangle = F_p^* \text{ or } \langle y \rangle = F_p^*\}, \tag{13}$$

where F_p^* is the multiplicative group of units and $\langle z \rangle$ denotes the set generated multiplicatively by $z \in F_p$.

Apart from evaluation at the points (14) and (15) below, the author has verified that the statement of Conjecture 6 is true for all evaluations of the Tutte polynomial in F_p for $3 < p \leq 37$.

$$\{(x, 1) \in F_p \times F_p : x \neq 1\}; \tag{14}$$

$$\{(x, y) \in F_p \times F_p : (x-1)(y-1) = 2\}. \tag{15}$$

For $p = 5$, the points listed in (12) and (13) account for all the points not shown to be easy by Theorem 2, except for the points in (14). All four points of (15) are easy for $p = 5$.

Note that for the restricted problem of evaluating the Tutte polynomial of *planar* graphs in F_p, the points of (15) will be easy by a theorem of [5]: evaluating the Tutte polynomial of planar graphs at the points $\{(x, y) \in \mathbb{C} \times \mathbb{C} : (x-1)(y-1) = 2\}$ is polynomial time.

Recall also that $T(G; 2, 1)$ counts forests in G and $(-1)^{|E|-r(E)}T(G; 0, 1-p)$ counts nowhere-zero p-flows in G when evaluation is in $\mathbb{Z}$. Interpreting evaluation in F_p as counting modulo a prime, the following question in particular arises from (14).

Problem 7 [1, §3.8] *For prime $p > 3$, is there a randomised polynomial-time algorithm for counting the number of forests of a graph modulo p? Can the number of nowhere-zero p-flows modulo p be found in random polynomial time?*

References

[1] J.D. Annan, The Complexity of Counting Problems, D.Phil. thesis, University of Oxford, 1994

[2] G.H. Hardy, and E.M. Wright, "An Introduction to the Theory of Numbers," 5th ed., Oxford University Press, Oxford, 1979

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

[4] L.G. Valiant, and V. Vazirani, NP is as easy as detecting unique solutions, *Theoret. Comp. Sc.* **47** (1986), 85-93

[5] D.L. Vertigan, The computational complexity of Tutte invariants for planar graphs, 1991 (to appear)

[6] 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

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