A Graph Polynomial for Independent Sets of Bipartite Graphs

Q. GE and D. ŠTEFANKOVIČ

Department of Computer Science, University of Rochester, Rochester, NY 14627–0226, USA
(e-mail: qge@cs.rochester.edu and stefanko@cs.rochester.edu)

We introduce a new graph polynomial that encodes interesting properties of graphs, for example, the number of matchings, the number of perfect matchings, and, for bipartite graphs, the number of independent sets (#BIS).

We analyse the complexity of exact evaluation of the polynomial at rational points and show a dichotomy result: for most points exact evaluation is #P-hard (assuming the generalized Riemann hypothesis) and for the rest of the points exact evaluation is trivial.

1. Introduction

Graph polynomials are a well-developed subject useful for analysing properties of graphs (see, *e.g.*, [13, 14] and [24]). Arguably the most intriguing graph polynomial is the Tutte polynomial [30, 31]. The partition function of the random cluster model from statistical mechanics provides a particularly simple definition: for a graph $G = (V, E)$ let

$$Z(G; q, \mu) = \sum_{S \subseteq E} q^{\kappa(S)} \mu^{|S|}, \tag{1.1}$$

where $\kappa(S)$ is the number of connected components of the graph (V, S). It is well known that the Tutte polynomial is obtained from Z by a simple transformation: see, *e.g.*, equation (4.4) below. The Tutte polynomial includes many graph polynomials as special cases, such as the chromatic polynomial, the flow polynomial, and the Potts model (see, *e.g.*, [34]).

Now we define our graph polynomial.

Table 1. Random cluster polynomials and R_2 polynomials for the claw graph, the path P_4 and the cycle C_3.

	Random cluster polynomial	R_2 polynomial
Claw graph	$(\mu+q)^3q$	$(\mu^3+3\mu^2+3\mu)q^2+1$
Path P_4	$(\mu+q)^3q$	$(\mu^3+\mu^2)q^4+(2\mu^2+3\mu)q^2+1$
Cycle C_3	$q^3+3\mu q^2+(\mu^3+3\mu^2)q$	$(\mu^3+3\mu^2+3\mu)q^2+1$

Definition. The R_2 polynomial of a graph $G=(V,E)$ is

$$R_2(G;q,\mu)=\sum_{S\subseteq E} q^{\mathrm{rk}_2(S)}\mu^{|S|}, \tag{1.2}$$

where $\mathrm{rk}_2(S)$ is the rank of the adjacency matrix of (V,S) over $\mathbb{F}_2$ (the field with 2 elements).

The definition of the R_2 polynomial looks very similar to the Tutte polynomial but they are quite different: for example, they count different invariants associated with a graph. To illustrate one difference between the random cluster polynomial and the R_2 polynomial, we provide a few small examples in Table 1. Note that P_4 and claw graphs (one vertex attached to 3 other vertices) have the same random cluster polynomial, whereas C_3 and claw graphs have the same R_2 polynomial.

The rank-based expansion of Tutte polynomial (see equation (4.3)) can be made similar to the R_2 polynomial in a different way: the exponent of $(x-1)$ can be expressed using the rank (over $\mathbb{F}_2$) of the incidence matrix of the subgraphs (see [1]). The two-variable interlace polynomial [1] has even more similarity to the R_2 polynomial in this respect: it is also defined using the rank (over $\mathbb{F}_2$) of the adjacency matrix of induced subgraphs (the main difference is that the two-variable interlace polynomial is a sum over subsets of vertices whereas the R_2 polynomial is a sum over subsets of edges).

The most interesting fact about the R_2 polynomial is that for bipartite graphs it encodes the number of independent sets (see Theorem 2.3 below). We are not aware of any other graph polynomial that encodes the number of independent sets in a non-obvious manner. (The independence polynomial of graph G is $I(G;x)=\sum_k s_k x^k$, where s_k is the number of independent sets of G of size k; here, obviously, $I(G,1)$ counts the number of independent sets of G.)

2. Our results

2.1. Invariants counted by the polynomial

Now we look at how $R_2(G;q,\mu)$ encodes the number of matchings, perfect matchings, and independent sets (in the bipartite case) of graphs.

Lemma 2.1. *Substituting $q=\mu^{-1/2}$ into equation* (1.2)*, we define*

$$P(G;\mu) := R_2(G;\mu^{-1/2},\mu)=\sum_{S\subseteq E(G)} \mu^{|S|-\mathrm{rk}_2(S)/2}.$$

Then $P(G;0)$ is the number of matchings in G.

Proof. Note that $\mathrm{rk}_2(S) \leqslant 2|S|$ (since adding an edge to S changes two entries in the adjacency matrix and hence can change rank by at most two), and $\mathrm{rk}_2(S) < 2|S|$ if S is not a matching (since the rank of the adjacency matrix of a star is $2 < 2|S|$, and adding further edges preserves the strict inequality). □

Lemma 2.2. *Let*

$$P(G;t,\mu) := t^{|V|}R_2(G;1/t,\mu) \quad \textit{and} \quad P_2(G;\mu) := \mu^{-|V|/2}P(G;0,\mu).$$

Then $P_2(G;0)$ is the number of perfect matchings of G.

Proof. Note that only subsets with full rank adjacency matrix contribute to $P(G;0,\mu)$, and then only the minimal cardinality subsets with full rank adjacency matrix contribute to $P_2(G;0)$. These subsets are exactly the perfect matchings. □

From now on we focus mainly on bipartite graphs. For a *bipartite* graph $G = (U \cup W, E)$ we let

$$R_2'(G;\lambda,\mu) = \sum_{S \subseteq E} \lambda^{\mathrm{rk}_2(S)}\mu^{|S|}, \tag{2.1}$$

where $\mathrm{rk}_2(S)$ is the rank of the *bipartite* adjacency matrix of $(U \cup W, S)$. Note that R_2' is just a reparametrization of R_2; more precisely,

$$R_2(G;\lambda,\mu) = R_2'(G;\lambda^2,\mu), \tag{2.2}$$

since the adjacency matrix contains 'two copies' of the bipartite adjacency matrix (one of them transposed). The reason for definition (2.1) is that it is simpler to work with the bipartite adjacency matrix for bipartite graphs.

In Section 3 we prove that R_2' counts the number of independent sets in bipartite graphs.

Theorem 2.3. *Let $G = (U \cup W, E)$ be a bipartite graph. The number of independent sets of G is given by*

$$2^{|U|+|W|-|E|}R_2'(G;1/2,1).$$

2.2. Complexity of exact evaluation of the polynomial

In our search for more invariants counted by the polynomial, we looked for points where it can be evaluated in polynomial time. The only interesting easily evaluated point found is $(\lambda,\mu) = (1/2,-1)$, which encodes the number of isolated vertices of G (see equation (4.2)).

We show in Section 4 that exact evaluation of the polynomial $R_2'(G;\lambda,\mu)$ is #P-hard at most points (λ,μ), assuming the validity of the generalized Riemann hypothesis (GRH).

Theorem 2.4. *Exact evaluation of R_2' at rational point (λ,μ) (i.e., computing the function $G \mapsto R_2'(G,\lambda,\mu)$) is*

(i) *polynomial-time computable when $\lambda \in \{0,1\}$ or $\mu = 0$ or $(\lambda,\mu) = (1/2,-1)$,*

(ii) *#P-hard when* $\lambda \notin \{0, 1, 1/2\}$ *and* $\mu \neq 0$*, assuming the GRH,*
(iii) *#P-hard when* $\lambda = 1/2$ *and* $\mu \notin \{0, -1\}$*, assuming the GRH.*

Theorem 2.4 fits the general theme of analysing the complexity of evaluating graph polynomials; related work includes that of Jaeger, Vertigan and Welsh [20] (for the Tutte polynomial), Bläser and Hoffmann [4] (for the two-variable interlace polynomial), and Makowsky [24] (providing a general framework for graph polynomials defined using second-order logic).

For the non-bipartite case we have the following classification. Exact evaluation of R_2 at rational point (λ, μ) is polynomial-time computable when $\mu = 0$ or $\lambda \in \{-1, 0, 1\}$; the $\lambda = -1$ case follows from the fact that a skew-symmetric matrix with zero diagonal has even rank over any field (the zero diagonal condition is redundant for fields of characteristic $\neq 2$). For any other rational λ and μ we get #P-hardness for evaluating the R_2 polynomial from Theorem 2.4 and (2.2) (again assuming the GRH). (Note that $(\lambda, \mu) \mapsto (\lambda^2, \mu)$ never maps to the easy case $(1/2, -1)$, since λ is rational. It would be nice to have hardness classification for evaluating R_2 and R_2' for, say, algebraic λ and μ.)

3. Independent sets in bipartite graphs

The problem of counting independent sets (#IS) in a graph is of interest in both computer science and statistical physics (independent sets are a special case of the so-called hard-core model: see, *e.g.*, [3]). Exact computation of #IS is #P-complete even for 3-regular planar bipartite graphs [32, 35]. A fully polynomial randomized approximation scheme (FPRAS) is known for graphs with maximum degree $\Delta \leqslant 5$, [23, 12, 33]. Unless RP=NP, an FPRAS does not exist for graphs with $\Delta \geqslant 6$ [28].

Now we focus on the problem of counting independent sets in bipartite graphs (#BIS). While for exact counting the complexity of #BIS and #IS is the same, the situation looks very different for approximate counting: for example, no inapproximability result is known for #BIS. Dyer, Goldberg, Greenhill and Jerrum [10] show that #BIS is complete with respect to approximation-preserving reductions (AP-reductions) in a sub-class of #P. Many problems have been shown to be equivalent (with respect to AP-reductions) to #BIS, for example, #DOWNSETS, #1P1NSAT [10], computing the partition function of a ferromagnetic Ising model with local fields [17], and counting the number of satisfying assignments of a class of Boolean CSP instances [11]. A pertinent negative result for #BIS is that Glauber dynamics (or, more generally, any chain whose states are independent sets and that flips at most $0.35n$ vertices in one step) cannot be used to efficiently sample random independent sets in a random 6-regular bipartite graphs on $n + n$ vertices [9].

The rest of this section is devoted to proving Theorem 2.3. It will be convenient to work with matrices instead of graphs. For two zero-one matrices A, B, we say $B \leqslant A$ if B corresponds to a subgraph of A, formally described as follows.

Definition. Let A, B be zero-one $n_1 \times n_2$ matrices. We say $B \leqslant A$ if $A_{ij} = 0$ implies $B_{ij} = 0$, for all $i \in [n_1]$ and $j \in [n_2]$. Let $\mathcal{C}_A$ be the set of zero-one $n_1 \times n_2$ matrices B such that $B \leqslant A$.

Let $\#_1(A)$ denote the number of ones in A (that is, the number of edges in the corresponding graph). The 'rank weighted subgraph' (RWS) problem rephrased for matrices is as follows.

Rank Weighted Matrices with $\lambda, \mu \geqslant 0$ (RWM(λ, μ)).
Input: an $n_1 \times n_2$ matrix A.
Output: $B \in \mathcal{C}_A$ with probability of $B \propto \lambda^{\mathrm{rk}_2(B)} \mu^{\#_1(B)}$.

The problem of sampling independent sets in bipartite graphs is as follows.

Bipartite Independent Sets (BIS).
Input: a bipartite graph $G = (U \cup W, E)$.
Output: a uniformly random independent set of G.

Before we show a connection between BIS and RWM$(1/2, 1)$, we remark that to sample bipartite independent sets it is enough to sample a subset of one side, say U, from the correct (marginal) distribution. We now describe this distribution in a setting which will be advantageous for the proof of Theorem 2.3.

We will represent an independent set by a pair of (indicator) vectors u, v (where $u \in \mathbb{F}_2^{n_1}$ and $v \in \mathbb{F}_2^{n_2}$).

Definition. We say that two vectors $\alpha, \beta \in \mathbb{F}_2^n$ *share a one* if there exists $i \in [n]$ such that $\alpha_i = \beta_i = 1$.

We will use the following simple fact.

Observation. Let $\alpha, \beta \in \mathbb{F}_2^n$. Let d be the number of ones in β.

- If α, β share a one then there are 2^{d-1} vectors $\beta' \leqslant \beta$ such that $\alpha^{\mathrm{T}} \beta' \equiv 0 \bmod 2$.
- If α, β do not share a one then there are 2^d vectors $\beta' \leqslant \beta$ such that $\alpha^{\mathrm{T}} \beta' \equiv 0 \bmod 2$.

Let $u \in \mathbb{F}_2^{n_1}$ be a vector. We would like to count the number of $v \in \mathbb{F}_2^{n_2}$ such that u, v is an independent set. Note that u, v is an independent set if and only if $v_j = 0$ for every $j \in [n_2]$ such that u and the jth column of A share a one. Let k be the number of columns of A that do not share a one with u. Then we have

$$u \in \mathbb{F}_2^{n_1} \text{ occurs in } 2^k \text{ independent sets.} \tag{3.1}$$

Thus to sample independent sets in a bipartite graph G with $n_1 \times n_2$ bipartite adjacency matrix A it is enough to sample $u \in \mathbb{F}_2^{n_1}$ with the probability of u proportional to 2^k, where k is the number of columns of A that do not share a one with u. We will call this distribution on u the marginal BIS distribution.

The following lemma shows a tight connection between BIS and RWM$(1/2, 1)$: given a sample from one distribution it is trivial to obtain a sample from the other one.

Lemma 3.1. *Let G be a bipartite graph with bipartite adjacency matrix A.*

- *Let u, v be a uniformly random independent set of G. Let B be a uniformly random matrix from the set $\{D \in \mathcal{C}_A \mid u^{\mathrm{T}} D \equiv 0 \bmod 2\}$. Then B is from the* RWM$(1/2, 1)$*-distribution.*
- *Let $B \in \mathcal{C}_A$ be a random matrix from the* RWM$(1/2, 1)$*-distribution. Let $u \in \mathbb{F}_2^{n_1}$ be a uniformly random vector from the left null space of B (that is, $\{\beta \in \mathbb{F}_2^{n_1} \mid \beta^{\mathrm{T}} B \equiv 0 \bmod 2\}$). Then u is from the marginal* BIS *distribution.*

Proof. Let Q be the set of u, B pairs such that $u^{\mathrm{T}} B \equiv 0 \bmod 2$ and $B \leqslant A$. Let ψ be the uniform distribution on Q. Note that ψ marginalized over u yields the RWM$(1/2, 1)$-distribution on $B \leqslant A$, where we are using the fact that a d-dimensional space (in this case the left null space of B) over $\mathbb{F}_2$ has 2^d elements. Formally,

$$P(B) = \sum_{u : u^{\mathrm{T}} B \equiv 0 \bmod 2} \frac{1}{|Q|} = \frac{2^{n_1 - \mathrm{rk}_2(B)}}{|Q|} = \frac{2^{-\mathrm{rk}_2(B)}}{R_2'(G; 1/2, 1)}. \tag{3.2}$$

Next we show that ψ marginalized over B yields the marginal BIS distribution. We compute the number of $B \leqslant A$ such that $u^{\mathrm{T}} B \equiv 0 \bmod 2$. Let us use the same k as in (3.1), that is, k is the number of columns of A that do not share a one with u.

Note that the columns of B can be chosen independently, and only if the column and u share a one is the number of choices (for that column) halved. Let $\#_1(A)$ be the number of ones in A. Thus

$$\text{there are } 2^{\#_1(A) - (n_2 - k)} \text{ choices of } B \leqslant A \text{ such that } u^{\mathrm{T}} B \equiv 0 \bmod 2. \tag{3.3}$$

Note that for fixed u the counts in (3.1) and (3.3) differ by a factor of $2^{\#_1(A) - n_2}$ (which is independent of u). Thus ψ marginalized over B yields the marginal BIS distribution on u. Formally

$$P(u) = \frac{2^{\#_1(A) - (n_2 - k)}}{|Q|} = \frac{2^k}{\#\mathrm{BIS}(G)}. \tag{3.4}$$

Note that this proves both claims of the lemma, since in both cases the u, B pair is from ψ (by first sampling from a marginal and then sampling the remaining variable), and the conclusion in both claims is a statement about the marginal of the remaining variable. □

Theorem 2.3 now follows from the proof of Lemma 3.1.

Proof of Theorem 2.3. Let Q be the set from the proof of Lemma 3.1. From (3.2) we obtain

$$|Q| = R_2'(G; 1/2, 1) 2^{n_1}. \tag{3.5}$$

From (3.4) we have that the number of independent sets of G is given by

$$\#\mathrm{BIS}(G) = \frac{|Q|}{2^{\#_1(A) - n_2}}. \tag{3.6}$$

Combining (3.5) and (3.6) we obtain the theorem. □

4. Exact evaluation of R_2' (proof of Theorem 2.4)

We will prove Theorem 2.4 in this section. Let $G = (V, E) = (U \cup W, E)$ be a bipartite graph. First we deal with the cases where exact evaluation of $R_2'(G; \lambda, \mu)$ is easy. For cases $\lambda \in \{0, 1\}$ and $\mu = 0$ we have

$$R_2'(G; 0, \mu) = R_2'(G; \lambda, 0) = 1 \quad \text{and} \quad R_2'(G; 1, \mu) = (1 + \mu)^{|E|}. \tag{4.1}$$

For $\lambda = 1/2$ and $\mu = -1$ we will show

$$R_2'(G; 1/2, -1) = 2^{|E|-|V|+t}, \tag{4.2}$$

where t is the number of isolated vertices in G (see the remark after Theorem 4.3 below).

For the hardness results we give reductions from the problem of evaluating the Tutte polynomial (to establish Theorem 2.4(ii)) and #BIS (to establish Theorem 2.4(iii)).

The Tutte polynomial of a graph $G = (V, E)$ is a polynomial in two variables x, y defined by

$$T(G; x, y) = \sum_{S \subseteq E} (x-1)^{\kappa(S)-\kappa(E)} (y-1)^{|S|-|V|+\kappa(S)}, \tag{4.3}$$

where $\kappa(S)$ is the number of connected components of the graph (V, S). The Tutte polynomial is closely related to the random cluster model (see, *e.g.*, [34]). Let $Z(G; q, \mu)$ be defined as in (1.1). We have

$$T(G; x, y) = (x-1)^{-\kappa(E)} (y-1)^{-|V|} Z(G; (x-1)(y-1), (y-1)), \tag{4.4}$$

where we assume $x \neq 1$ and $y \neq 1$.

We are going to use the following result on the complexity of exact evaluation of the Tutte polynomial. The hardness results of [20] are for multigraphs (that is, parallel edges are allowed). However, our reductions turn multigraphs into (simple) graphs.

Theorem 4.1 ([20]). *Exact evaluation of the Tutte polynomial* (*on multigraphs*) *is #P-hard for all rational numbers x, y except when*

(i) $(x-1)(y-1) = 1$, *or*
(ii) (x, y) *equals* $(1, 1)$, $(-1, -1)$, $(0, -1)$ *or* $(-1, 0)$.

Theorem 2.4(ii) will be proved by reducing from exact evaluation of the Tutte polynomial. We prove the following lemma in Section 4.1.

Lemma 4.2. *Assuming the validity of the GRH, exact evaluation of the Tutte polynomial* (*for multigraphs*) *at x, y is polynomial-time Turing-reducible to exact evaluation of R_2' polynomial* (*for simple graphs*) *at λ, μ, when*

$$(x-1)(y-1) = 1/\lambda - 1, \quad y - 1 = \mu^2, \quad \lambda \notin \{0, 1\}, \quad \textit{and} \quad \mu \neq 0. \tag{4.5}$$

Assuming the GRH, by Lemma 4.2 and Theorem 4.1, we have that exact evaluation of R_2' at rational point (λ, μ) is #P-hard when $\lambda \notin \{0, 1/2, 1\}$ and $\mu \neq 0$. We do not get #P-hardness for $\lambda = 1/2$ since the reduction is from the Tutte polynomial at

$(x-1)(y-1)=1$, which is polynomial-time computable (Theorem 4.1(i)). (The other easy cases of the Tutte polynomial have no impact since $y=1$ implies $\mu=0$ and $y\in\{0,-1\}$ implies that μ is not real.) We have proved Theorem 2.4(ii).

Now we prove Theorem 2.4(iii) (the proof of the main lemmas is deferred to later sections). To show #P-hardness of exact evaluation of $R_2'(G;1/2,\mu)$ for $\mu\notin\{-1,0\}$, we prove a connection between R_2' and the 'permissive version of #BIS' (#PBIS) introduced in [17]; #PBIS is a generalization of #BIS where the weight of a set of vertices is determined by the number of pairs of neighbouring vertices that are both in the set (in #BIS the weight is zero raised to the number of such pairs).

#Permissive Bipartite Independent Sets with parameter η (#PBIS(η)).
Input: a bipartite graph $G=(U\cup W,E)$.
Output: the quantity

$$\#\mathrm{PBIS}(G;\eta)=\sum_{\sigma:U\cup W\to\{0,1\}}(1+\eta)^{w(\sigma)}(1-\eta)^{|E|-w(\sigma)},\tag{4.6}$$

where $w(\sigma)$ is the number of edges in E with both endpoints labelled 1 by σ.

(We are using a parametrization different from that of [17]: our η and their γ are connected by $\gamma^2=(1+\eta)/(1-\eta)$.)

Note that

$$\#\mathrm{BIS}(G)=2^{|E|}\#\mathrm{PBIS}(G;-1).$$

The following result is a generalization of Theorem 2.3 and shows that R_2' encodes #PBIS(η) as well. The proof is deferred to Section 4.2.

Theorem 4.3. *Let $G=(V,E)=(U\cup W,E)$ be a bipartite graph. Then*

$$\#\mathrm{PBIS}(G;\eta)=2^{|V|}R_2'(G;1/2,-\eta).$$

Note that $\#\mathrm{PBIS}(G;1)=2^{|E|+t}$, where t is the number of isolated vertices of G (since the other vertices have to be labelled 1 by σ). This implies (4.2).

The following result on #PBIS(η) will be proved in Section 4.3.

Lemma 4.4. *Assuming the validity of the GRH,* #BIS *is polynomial-time Turing-reducible to* #PBIS(η) *with η a rational number and $\eta\notin\{\pm1,0\}$.*

Theorem 2.4(iii) follows from Theorem 4.3, Lemma 4.4 and the fact that exact computation of #BIS is #P-complete [27].

4.1. Reducing the Tutte polynomial to the R_2' polynomial (proof of Lemma 4.2)

We will focus on bipartite graphs $G=(U\cup W,E)$ such that vertices in partition W have degree at most 2 (a natural operation that produces such graphs is a 2-*stretch*, that is, replacement of each edge with a path of length 2).

Let $G = (U \cup W, E)$ be a bipartite graph with max-degree in W bounded by 2. We call a connected component $C = (U_C \cup W_C, E_C)$ of G *pure* if every vertex in W_C has degree 2 in C. A component that is not pure will be called *mixed*. The evaluation of the R'_2 polynomial in G can be expressed using pure connected components as follows.

Lemma 4.5. *For every bipartite graph $G = (U \cup W, E)$ such that the degree of each vertex in W is bounded by 2,*

$$R'_2(G; \lambda, \mu) = \sum_{S \subseteq E} \lambda^{|U| - \kappa'(S)} \mu^{|S|},$$

where $\kappa'(S)$ is the number of pure connected components in $(U \cup W, S)$.

Before proving Lemma 4.5 we need the following characterization of the rank of bipartite adjacency matrices over $\mathbb{F}_2$.

Lemma 4.6. *Let $G = (U \cup W, E)$ be a connected bipartite graph with max-degree in W bounded by 2. Let B be the adjacency matrix of G. Then*

$$\mathrm{rk}_2(B) = \begin{cases} |U| & \text{if there is a vertex of degree 1 in } W, \\ |U| - 1 & \text{otherwise.} \end{cases}$$

Proof. Let $x \in \mathbb{F}_2^U$ be a solution of the linear system $x^{\mathrm{T}} B = 0$. Let U_i be the set of vertices $u \in U$ such that $x_u = i$, for $i = 0, 1$. Note that no vertex $v \in W$ has neighbours in both U_0 and U_1 (otherwise $(x^{\mathrm{T}} B)_v = 1$). Thus for G to be connected either $x = 0$ or $x = 1$. If there is a vertex of degree 1 in W then $x = 1$ is not a solution, and hence $\mathrm{rk}_2(B) = |U|$. On the other hand, if all vertices in W have degree 2 then $x = 1$ is a solution and hence $\mathrm{rk}_2(B) = |U| - 1$. □

Now we prove Lemma 4.5.

Proof of Lemma 4.5. We will show that

$$\mathrm{rk}_2(S) = |U| - \kappa'(S), \tag{4.7}$$

where $\mathrm{rk}_2(S)$ is the rank (over $\mathbb{F}_2$) of B, the bipartite adjacency matrix of $(U \cup W, S)$, and $\kappa'(S)$ is the number of pure connected components of $(U \cup W, S)$.

Note that B has a block structure with a block for each connected component. The rank is the sum of the ranks of the blocks. Equation (4.7) now follows from Lemma 4.6. □

We now lay groundwork for the proof of Lemma 4.2. We use the following construction in the reduction. Given a (multi-) graph $H = (V_H, E_H)$ and a bipartite graph $\Upsilon = (U_\Upsilon \cup W_\Upsilon, E_\Upsilon)$ with a specific vertex $u \in U_\Upsilon$, we construct a bipartite graph G from H and Υ as follows. Let $\hat{H} = (V_H \cup W_{\hat{H}}, E_{\hat{H}})$ be the 2-stretch of H, where $W_{\hat{H}}$ are the 'new' vertices. For each vertex v in V_H we identify v with u in a copy of Υ (thus we have $|V_H|$ copies

of Υ). We call the graph G the *stretch-sum* of H and (Υ, u). Note that if W_Υ contains only vertices of degree at most 2 then the partition of G containing $W_{\hat{H}}$ contains only vertices of degree at most 2.

We define two functions related to R_2'.

Definition. Let $\lambda, \mu \in \mathbb{R}$. Let $\Upsilon = (U \cup W, E)$ be a bipartite graph with a specific vertex $u \in U$. Assume that the max-degree in W is bounded by 2. We define

$$Z_p'(\Upsilon; \lambda, \mu) = \sum_S \lambda^{-\kappa'(S)} \mu^{|S|}, \tag{4.8}$$

where the sum is over all $S \subseteq E$ such that u is in a pure connected component of $(U \cup W, S)$, and $\kappa'(S)$ is the number of pure connected components of $(U \cup W, S)$.

Similarly, we define

$$Z_m'(\Upsilon; \lambda, \mu) = \sum_S \lambda^{-\kappa'(S)} \mu^{|S|}, \tag{4.9}$$

where the sum is over all sets $S \subseteq E$ such that u is in a mixed connected component of $(U \cup W, S)$.

The following lemma provides a connection between the random cluster partition function Z of H and the R_2' polynomial of G for rational λ and μ.

Lemma 4.7. *Fix rational $\lambda \notin \{0, 1\}$ and rational $\mu \neq 0$. Let p be a prime such that $\lambda \in \mathbb{Z}_p^*$. Let $\Upsilon = (U \cup W, E)$ be a bipartite graph with a specific vertex $u \in U$, such that the max-degree in W bounded by 2. Suppose Υ satisfies*

$$\begin{aligned} X &:= \lambda Z_p'(\Upsilon; \lambda, \mu) \not\equiv 0 \bmod p, \\ Y &:= Z_m'(\Upsilon; \lambda, \mu) + \lambda Z_p'(\Upsilon; \lambda, \mu) \equiv 0 \bmod p. \end{aligned} \tag{4.10}$$

Let G be the stretch-sum of the (multi-) graph $H = (V_H, E_H)$ and (Υ, u). Then

$$R_2'(G; \lambda, \mu) \equiv \lambda^{|V_H| \cdot |U|} X^{|V_H|} Z(H; 1/\lambda - 1, \mu^2) \bmod p, \tag{4.11}$$

where $Z(H; 1/\lambda - 1, \mu^2)$ is defined in (1.1).

Proof. Let $\hat{H} = (V_{\hat{H}}, E_{\hat{H}})$ be the 2-stretch of H. Note that $\hat{H}$ is a subgraph of $G = (V_G, E_G)$. Let $S_0 \subseteq E_{\hat{H}}$. Let Λ_{S_0} be a family of subsets $S \subseteq E_G$ such that $S \cap E_{\hat{H}} = S_0$. Now, we evaluate

$$\sum_{S \in \Lambda_{S_0}} \lambda^{-\kappa'(S)} \mu^{|S|} \tag{4.12}$$

modulo p.

Claim 1. *If $(V_{\hat{H}}, S_0)$ has no mixed connected component, then*

$$(4.12) \equiv (\lambda^{-1} - 1)^{\kappa(S_0)} \mu^{|S_0|} X^{|V_H|} \bmod p,$$

where $\kappa(S_0)$ is the number of connected components of $(V_{\hat{H}}, S_0)$; otherwise,

$$(4.12) \equiv 0 \bmod p.$$

Proof of Claim 1. Equation (4.12) can be rewritten as a product, where each term in the product corresponds to a connected component of $(V_{\hat{H}}, S_0)$ (since each connected component with the copies of Υ attached to it influences $\kappa'(S)$ independently). Thus

$$(4.12) = \prod_C \Phi_C,$$

where for each connected component $C = (V_C, E_C)$ in $(V_{\hat{H}}, S_0)$ such that there are k copies of Υ (we refer to the copies as $\Upsilon_1, \ldots, \Upsilon_k$ and to their special vertices as $u_1, \ldots, u_k$) attached to it, that is,

$$\Phi_C = \sum_{S_1 \subseteq E_{\Upsilon_1}} \cdots \sum_{S_k \subseteq E_{\Upsilon_k}} \lambda^{-\kappa'(\bigcup_{i\in[k]} S_i \cup E_C)} \mu^{|E_C| + \sum_{i\in[k]} |S_i|}. \tag{4.13}$$

Let $A_{i,0}$ be the set of S_i such that u_i is in a mixed component of (V_{Υ_i}, S_i) and let $A_{i,1} = 2^{E_{\Upsilon_i}} \setminus A_{i,0}$. Equation (4.13) can be written as

$$\Phi_C = \sum_{x_1=0}^{1} \cdots \sum_{x_k=0}^{1} \sum_{S_1 \in A_{1,x_1}} \cdots \sum_{S_k \in A_{k,x_k}} \lambda^{-\kappa'(\bigcup_{i\in[k]} S_i \cup E_C)} \mu^{|E_C| + \sum_{i\in[k]} |S_i|}. \tag{4.14}$$

We have

$$\kappa'\left(\bigcup_{i\in[k]} S_i \cup E_C\right) = \sum_{i\in[k]} \kappa'_i(S_i) - \sum_{i=1}^{k} x_i + \ell,$$

where $\ell = 1$ if $x_1 = \cdots = x_k = 1$ and $C = (V_C, E_C)$ is a pure connected component of $(V_{\hat{H}}, S_0)$, and $\ell = 0$ otherwise. Thus

$$\begin{aligned} &\sum_{S_1 \in A_{1,x_1}} \cdots \sum_{S_k \in A_{k,x_k}} \lambda^{-\kappa'(\bigcup_{i\in[k]} S_i \cup E_C)} \mu^{|E_C| + \sum_{i\in[k]} |S_i|} \\ &\quad = \lambda^{-\ell} \mu^{|E_C|} \sum_{S_1 \in A_{1,x_1}} \cdots \sum_{S_k \in A_{k,x_k}} \prod_{i=1}^{k} \lambda^{-\kappa'_i(S_i) + x_i} \mu^{|S_i|} = \lambda^{-\ell} \mu^{|E_C|} X^{k'} (Y - X)^{k-k'}, \end{aligned} \tag{4.15}$$

where $k' = x_1 + \cdots + x_k$.

Plugging (4.15) into (4.14), we obtain

$$\Phi_C = \mu^{|E_C|} Y^k + L, \tag{4.16}$$

where $L = (1/\lambda - 1)\mu^{|E_C|} X^k$ if C is a pure component of $(V_{\hat{H}}, S_0)$ and 0 otherwise. Evaluating (4.16) modulo p (using (4.10)), we obtain

$$\Phi_C \equiv \begin{cases} 0 \bmod p & \text{if } C \text{ is a mixed component of } (V_{\hat{H}}, S_0), \\ (1/\lambda - 1)\mu^{|E_C|} X^k \bmod p & \text{otherwise.} \end{cases}$$

Thus (4.12) is zero modulo p if there is a mixed component C in $(V_{\hat{H}}, S_0)$. Assume now that all components of $(V_{\hat{H}}, S_0)$ are pure. The total number of edges in the components is

$|S_0|$, the total number of copies of Υ in the components is $|V_H|$, and hence

$$(4.12) \equiv (1/\lambda - 1)^{\kappa(S_0)} \mu^{|S_0|} X^{|V_H|} \bmod p. \qquad \square$$

Now we use Claim 1 to prove (4.11). Note that by Lemma 4.5,

$$R'_2(G;\lambda,\mu) = \lambda^{|V_H|\cdot|U|} \sum_{S_0 \subseteq E_{\hat{H}}} \sum_{S \in \Lambda_{S_0}} \lambda^{-\kappa'(S)} \mu^{|S|}, \tag{4.17}$$

where $\kappa'(S)$ is the number of pure connected components of (V_G, S).

Note that by Claim 1, if S_0 contains a mixed component then the inner sum in (4.17) is 0 modulo p. Thus to evaluate (4.17) modulo p it is enough to sum over S_0 which contain only pure components. Each such S_0 is obtained from exactly one $S' \subseteq E_H$ by 2-stretching. Note $(V_{\hat{H}}, S_0)$ has the same number of connected components as (V_H, S'), and $|S_0| = 2|S'|$. Thus

$$\begin{aligned} R'_2(G;\lambda,\mu) &\equiv \lambda^{|V_H|\cdot|U|} X^{|V_H|} \sum_{S' \subseteq E_H} (1/\lambda - 1)^{\kappa(S')} \mu^{2|S'|} \\ &\equiv \lambda^{|V_H|\cdot|U|} X^{|V_H|} Z(H; 1/\lambda - 1, \mu^2) \bmod p. \qquad \square \end{aligned}$$

We use different Υ for different values of μ in the reduction. When $\mu \neq -2$ we let Υ_1 be the bipartite graph with bipartition $U = \{u_0, u_1\}$, $W = \{v_i \mid 0 \leqslant i \leqslant k\}$ and $k+2$ edges: edge $\{u_0, v_0\}$, and an edge between u_1 and each v_i, for $0 \leqslant i \leqslant k$. The specific vertex of Υ_1 is u_0. By elementary counting, we have

$$\begin{aligned} \lambda Z'_p(\Upsilon_1;\lambda,\mu) &= (\mu+1)^{k+1} + \mu^2 + \lambda^{-1} - 1, \\ \lambda Z'_p(\Upsilon_1;\lambda,\mu) + Z'_m(\Upsilon_1;\lambda,\mu) &= (\mu+1)((\mu+1)^{k+1} + \lambda^{-1} - 1). \end{aligned} \tag{4.18}$$

When $\mu = -2$ we let Υ_2 be the bipartite graph with bipartition $U = \{u_0, u_1, u_2\}$, $W = \{v_i \mid 0 \leqslant i \leqslant 2k\}$ and $4k+2$ edges: $\{u_0, v_0\}$, $\{u_1, v_0\}$, and a complete bipartite graph between $U \setminus \{u_0\}$ and $W \setminus \{v_0\}$. The specific vertex of Υ_2 is u_0. By elementary counting, we have

$$\begin{aligned} \lambda Z'_p(\Upsilon_2;\lambda,-2) &= \lambda^{-2} + 5^{2k}\lambda^{-1} - 3 + 3 \cdot 5^{2k} + \lambda^{-1}, \\ \lambda Z'_p(\Upsilon_2;\lambda,-2) + Z'_m(\Upsilon_2;\lambda,-2) &= -\lambda^{-2} - 5^{2k}\lambda^{-1} - 1 + 5^{2k} + 3\lambda^{-1}. \end{aligned} \tag{4.19}$$

Fix rational $\lambda \notin \{0, 1\}$ and $\mu \neq 0$. We want to find sufficiently many primes such that there is some integer k for which (4.18) satisfies (4.10) (when $\mu \neq -2$) or (4.19) satisfies (4.10) (when $\mu = -2$). We need the following result on the density of primes.

Lemma 4.8 ([25, 26, 29]). *Let $r, q \in \mathbb{Q}^*$ and $q \neq \pm 1$. The density (inside the set of all primes) of primes p, such that*

$$q^k \equiv r \bmod p$$

can be satisfied for some integer k, is a positive constant, assuming the GRH.

Lemma 4.8 immediately yields the following two corollaries.

Corollary 4.9. *Fix rational $\lambda \notin \{0,1\}$ and rational $\mu \notin \{0,-2\}$. The density (inside the set of all primes) of the primes p, such that there is an integer k for which* (4.18) *satisfies* (4.10)*, is a positive constant, assuming the GRH.*

Proof. If $\mu = -1$, then to ensure (4.18) satisfies (4.10) it is sufficient to have $\lambda^{-1} \not\equiv 0 \bmod p$. Thus, for all but a finite number of primes, and for all positive integers k, (4.18) satisfies (4.10).

Now assume $\mu \neq -1$. To ensure (4.18) satisfies (4.10), it is sufficient to have

$$\begin{aligned} (\mu+1)^{k+1} + \lambda^{-1} - 1 &\equiv 0 \bmod p, \\ \mu &\not\equiv 0 \bmod p. \end{aligned} \tag{4.20}$$

The corollary follows from Lemma 4.8 (and the fact that the number of primes such that $\mu \equiv 0 \bmod p$ is finite). □

Corollary 4.10. *Fix rational $\lambda \notin \{0,1\}$ and rational $\mu = -2$. The density (inside the set of all primes) of the primes p, such that there is an integer k for which* (4.19) *satisfies* (4.10)*, is a positive constant, assuming the GRH.*

Proof. We claim that if

$$\begin{aligned} (\lambda^{-2} - 3\lambda^{-1} + 1)(1-\lambda^{-1})^{-1} &\equiv 25^k \bmod p, \\ 1 - \lambda^{-1} &\not\equiv 25^k \bmod p, \end{aligned} \tag{4.21}$$

then (4.19) satisfies (4.10). The first equation in (4.21) ensures the second equation in (4.10) is satisfied, and the first and second equations in (4.21) imply the first equation in (4.10) is satisfied.

By Lemma 4.8 the density of primes that ensure the first equation in (4.21) is satisfied is positive. Solving

$$(\lambda^{-2} - 3\lambda^{-1} + 1)(1-\lambda^{-1})^{-1} \equiv 1 - \lambda^{-1} \bmod p,$$

we obtain $\lambda^{-1} \equiv 0 \bmod p$, and hence the second equation in (4.21) is automatically satisfied. □

Proof of Lemma 4.2. Let x, y, λ, μ be rational numbers such that (4.5) is satisfied. Suppose $\lambda = a/b$ and $\mu = c/d$ with $a, b, c, d \in \mathbb{Z}^*$, $\gcd(a,b) = 1$, and $\gcd(c,d) = 1$.

Suppose we want to evaluate the Tutte polynomial for $H = (V_H, E_H)$ at x, y. Let $n := |V_H|$ and $m := |E_H|$. By (4.4), to evaluate $T(H; x, y)$, we can instead evaluate $Z(H; 1/\lambda - 1, \mu^2)$ (note that $\lambda \neq 1$ implies $x \neq 1$ and $y \neq 1$ and hence (4.4) applies). Recall that

$$Z(H; 1/\lambda - 1, \mu^2) = \sum_{S \subseteq E_H} (1/\lambda - 1)^{\kappa(S)} \mu^{2|S|} = \frac{L}{a^n d^{2m}}, \tag{4.22}$$

where

$$L = \sum_{S \subseteq E_H} (b-a)^{\kappa(S)} a^{n-\kappa(S)} c^{2|S|} d^{2m-2|S|}.$$

Note that $L \in \mathbb{Z}$ and $|L| \leqslant 2^m |b-a|^n a^n c^{2m} d^{2m}$.

We now prove the case $\mu \neq -2$. For the case $\mu = -2$, the proof is similar (by using Υ_2 and Corollary 4.10).

We choose n^3 primes $p_1, \ldots, p_{n^3}$ such that

- $a, b, c, d \not\equiv 0 \bmod p_i$, and $a + b \not\equiv 0 \bmod p_i$, for each $i \in [n^3]$,
- there is some integer k for which (4.20) is satisfied with $p = p_i$, for each $i \in [n^3]$,
- $p_i = O(n^4)$ for $i \in [n^3]$, and
- $\prod_{i=1}^{n^3} p_i > 2^{m+1}|b-a|^n a^n c^{2m} d^{2m}$.

By Corollary 4.9, these primes exist. We can find them in time polynomial in n by exhaustive search.

For each p_i, let $0 < k_i < p_i$ be an integer for which (4.18) satisfies (4.10) with $p = p_i$ (by Fermat's Little Theorem, if k_i is a solution, then $k_i + t(p_i - 1)$ is a solution as well, for every $t \in \mathbb{Z}$). Again, we can find them in time polynomial in n by exhaustive search.

We use Υ_1 with $k = k_i$ as above. Let G_i be the stretch-sum of H and (Υ_1, u_0) as above. Note that G_i has size polynomial in n since $k_i = O(n^4)$. By Lemma 4.7 and (4.22), we have

$$L \equiv a^n d^{2m} \lambda^{-2n} X^{-n} R_2'(G_i; \lambda, \mu) \bmod p_i,$$

where $X = \lambda Z_p'(\Upsilon_1; \lambda, \mu)$. We can make a query to the oracle to obtain the rational number $R_2'(G_i; \lambda, \mu)$ and can thus compute $L \bmod p_i$ in polynomial time for each $i \in [n^3]$. By the Chinese Remainder Theorem, we can compute L in time polynomial in n (see, *e.g.*, [2], p.106). □

4.2. Reducing #PBIS to the R_2' polynomial (proof of Theorem 4.3)

Now we show the connection between #PBIS and the R_2' polynomial; the proof of Theorem 4.3 is similar to the proof of the high-temperature expansion of the Ising model (see, *e.g.*, [21]).

Proof of Theorem 4.3.

$$\begin{aligned} \#\mathrm{PBIS}(G; \eta) &= \sum_{\sigma: U \cup W \to \{0,1\}} (1+\eta)^{w(\sigma)} (1-\eta)^{|E| - w(\sigma)} \\ &= \sum_{\sigma: U \cup W \to \{0,1\}} \prod_{\{u,v\} \in E} (1 + \eta \chi(\sigma(u), \sigma(v))), \end{aligned} \tag{4.23}$$

where

$$\chi(\sigma(u), \sigma(v)) = \begin{cases} 1 & \text{if } \sigma(u) = \sigma(v) = 1, \\ -1 & \text{otherwise.} \end{cases} \tag{4.24}$$

Let

$$\Psi_{S,\sigma_1,\sigma_2} := \prod_{\{u,v\} \in S} \chi(\sigma_1(u), \sigma_2(v)) \quad \text{and} \quad \Psi_{S,\sigma_1} := \sum_{\sigma_2: W \to \{0,1\}} \Psi_{S,\sigma_1,\sigma_2}.$$

Expanding the product in (4.23) and changing the order of summation yields

$$\begin{aligned}(4.23) &= \sum_{\sigma:U\cup W\to\{0,1\}} \sum_{S\subseteq E} \prod_{\{u,v\}\in S} \eta\chi(\sigma(u),\sigma(v)) \\ &= \sum_{S\subseteq E} \eta^{|S|} \sum_{\sigma:U\cup W\to\{0,1\}} \prod_{\{u,v\}\in S} \chi(\sigma(u),\sigma(v)) \\ &= \sum_{S\subseteq E} \eta^{|S|} \sum_{\sigma_1:U\to\{0,1\}} \Psi_{S,\sigma_1}. \qquad (4.25)\end{aligned}$$

Let $N_S(v)$ denote the set of neighbours of v in the subgraph $(U\cup W,S)$. Fix S and $\sigma_1 : U\to\{0,1\}$. We say that a pair S,σ_1 is good if for every $v\in W$ the number of vertices $u\in N_S(v)$ such that $\sigma_1(u)=1$ is even. A pair which is not good will be called bad.

Claim 2. *$\Psi_{S,\sigma_1} = 2^{|W|}(-1)^{|S|}$ if the pair S,σ_1 is good; and $\Psi_{S,\sigma_1}=0$ if the pair S,σ_1 is bad.*

Proof of Claim 2. Suppose that σ_2 and σ_2' differ only in the value assigned to $v\in W$. For every $u\in N_S(v)$ we have

$$\chi(\sigma_1(u),\sigma_2(v)) = \begin{cases} \chi(\sigma_1(u),\sigma_2'(v)) & \text{if } \sigma_1(u)=0, \\ -\chi(\sigma_1(u),\sigma_2'(v)) & \text{if } \sigma_1(u)=1. \end{cases}$$

Hence,

$$\Psi_{S,\sigma_1,\sigma_2} = \begin{cases} -\Psi_{S,\sigma_1,\sigma_2'} & \text{if } |\{u\in N_S(v)\,|\,\sigma_1(u)=1\}| \text{ is odd}, \\ \Psi_{S,\sigma_1,\sigma_2'} & \text{otherwise.} \end{cases}$$

If the pair S,σ_1 is bad, then there is a vertex $v\in W$ such that $|\{u\in N_S(v)\,|\,\sigma_1(u)=1\}|$ is odd. We can partition the $W\to\{0,1\}$ mappings into pairs σ_2,σ_2' that differ only in the label of v. For each pair, we have $\Psi_{S,\sigma_1,\sigma_2}+\Psi_{S,\sigma_1,\sigma_2'}=0$, and thus $\Psi_{S,\sigma_1}=0$.

If the pair S,σ_1 is good, then each $\Psi_{S,\sigma_1,\sigma_2}$ contributes the same value $(-1)^{|S|}$. Since there are $2^{|W|}$ mappings from W to $\{0,1\}$, we have $\Psi_{S,\sigma_1}=2^{|W|}(-1)^{|S|}$. □

Claim 3. *Fix $S\subseteq E$; the number of $\sigma_1:U\to\{0,1\}$ such that the pair S,σ_1 is good is $2^{|U|-\mathrm{rk}_2(S)}$, where $\mathrm{rk}_2(S)$ is the rank (over $\mathbb{F}_2$) of the bipartite adjacency matrix of $(U\cup W,S)$.*

Proof of Claim 3. Let B be the bipartite adjacency matrix of $(U\cup W,S)$. Note that the pair S,σ_1 is good if and only if

$$\sigma_1^{\mathrm{T}} B \equiv 0 \bmod 2$$

(we view σ_1 as a vector with $(\sigma_1)_v=\sigma_1(v)$). The claim follows from the fact that the number of vectors $\alpha\in\{0,1\}^{|U|}$ such that $\alpha^{\mathrm{T}}B\equiv 0 \bmod 2$ is $2^{|U|-\mathrm{rk}_2(B)}$. □

By Claim 2 and Claim 3, (4.25) equals

$$\sum_{S\subseteq E} 2^{|U|+|W|-\mathrm{rk}_2(S)}(-\eta)^{|S|} = 2^{|U|+|W|}R_2'(G;1/2,-\eta).$$ □

4.3. Reducing #BIS to #PBIS (proof of Lemma 4.4)

We use the following construction in the proof of Lemma 4.4. Let H be a bipartite graph with a special vertex h. Given a graph $G = (V, E)$ and a prime p we construct a bipartite graph G' by replacing each edge $e \in E$ by $p-1$ copies of H. For every vertex $v \in V$ and every edge e adjacent to v, we add edges between v and the special vertices of the copies of H for e.

Let $P_0(\eta)$ be the part of $\#\mathrm{PBIS}(H;\eta)$ where the label of h is 0 (that is, in the sum (4.6) we only take the σ that label h by zero). Similarly, let $P_1(\eta)$ be the part of $\#\mathrm{PBIS}(H;\eta)$ where the label of h is 1. We would like $P_0(\eta)$ and $P_1(\eta)$ to be such that we can recover the number of independent sets of G modulo p from $\#\mathrm{PBIS}(G';\eta) \bmod p$.

Lemma 4.11. *Let $p \geqslant 3$ be a prime, let H be a bipartite graph, and let η be a rational number such that $\eta(1+\eta) \in \mathbb{Z}_p^*$ and*

$$\begin{aligned}(1-\eta)^2 P_0(\eta) + (1+\eta)^2 P_1(\eta) &\equiv 0 \bmod p,\\ P_1(\eta) &\not\equiv 0 \bmod p.\end{aligned} \tag{4.26}$$

Let $G = (V, E)$ be a graph and let $G' = (V', E')$ be the graph constructed above using p and H (where $P_0(\eta)$ and $P_1(\eta)$ correspond to H). Then the number of independent sets of G is congruent to $\#\mathrm{PBIS}(G';\eta) \bmod p$.

Proof. We are going to evaluate

$$\#\mathrm{PBIS}(G';\eta) = \sum_{\sigma: V' \to \{0,1\}} \prod_{\{u,v\} \in E'} (1 + \eta\chi(\sigma(u), \sigma(v))) \tag{4.27}$$

modulo p (where χ is given by (4.24)).

For $\varsigma : V \to \{0,1\}$, let C_ς be the set of assignments $V' \to \{0,1\}$ that assign label $\varsigma(s)$ to vertex s (for every $s \in V$). Now we evaluate

$$\sum_{\sigma \in C_\varsigma} \prod_{\{u,v\} \in E'} (1 + \eta\chi(\sigma(u), \sigma(v))). \tag{4.28}$$

Note that each copy of H influences its own set of terms in the product in (4.28). Thus the sum in (4.28) turns into the product

$$(4.28) = \prod_{\{s,t\} \in E} \Psi(\varsigma(s), \varsigma(t)), \tag{4.29}$$

where $\Psi(x, y)$ is defined as follows:

$$\begin{aligned}\Psi(x,y) = [&(1+\eta\chi(x,0))(1+\eta\chi(y,0))P_0(\eta)\\ &+(1+\eta\chi(x,1))(1+\eta\chi(y,1))P_1(\eta)]^{p-1}.\end{aligned} \tag{4.30}$$

The first term in (4.30) corresponds to assigning zero to the special vertex and the second term corresponds to assigning one to the special vertex.

Now we evaluate $\Psi(x, y)$ for $x, y \in \{0,1\}$.

Case 1: $x = y = 1$. We have

$$\Psi(1,1) = \big((1-\eta)^2 P_0(\eta) + (1+\eta)^2 P_1(\eta)\big)^{p-1} \equiv 0 \bmod p, \tag{4.31}$$

where the congruence follows from the assumption (4.26).

Case 2: $x = y = 0$. We have

$$\Psi(0,0) = \big((1-\eta)^2 P_0(\eta) + (1-\eta)^2 P_1(\eta)\big)^{p-1} \equiv 1 \bmod p, \tag{4.32}$$

where in the congruence we used (4.26) and Fermat's Little Theorem (note that the difference of the arguments in (4.31) and (4.32) is $4\eta P_1(\eta)$).

Case 3: $x = 1, y = 0$ (the case $x = 0, y = 1$ is the same). We have

$$\Psi(1,0) = \big((1-\eta)^2 P_0(\eta) + (1-\eta)(1+\eta) P_1(\eta)\big)^{p-1} \equiv 1 \bmod p, \tag{4.33}$$

where in the congruence we used (4.26) and Fermat's Little Theorem (note that the difference of the arguments in (4.31) and (4.33) is $2\eta(1+\eta)P_1(\eta)$).

From (4.31), (4.32), and (4.33) we obtain that (4.29) modulo p is 1 if ς corresponds to an independent set of G and is zero otherwise. Thus we have

$$\#\mathrm{PBIS}(G';\eta) \equiv \sum_{\varsigma \in V \to \{0,1\}} \prod_{\{s,t\} \in E} \Psi(\varsigma(s), \varsigma(t)) \equiv \#\mathrm{BIS}(G) \bmod p. \qquad \square$$

Now we use the following gadgets for H in Lemma 4.11 to prove Lemma 4.4. For $\eta \neq 2$ we take H to be the star with k leaves (that is, $K_{1,k}$) where the special vertex h is the centre of the star. Note that $P_0(\eta) = 2^k(1-\eta)^k$ and $P_1(\eta) = (1-\eta+1+\eta)^k = 2^k$. The condition (4.26) becomes

$$(1-\eta)^{k+2} + (1+\eta)^2 \equiv 0 \bmod p. \tag{4.34}$$

We want to find sufficiently many primes p such that (4.34) can be satisfied for some integer k. This is a corollary of Lemma 4.8, taking

$$r = -\left(\frac{1+\eta}{1-\eta}\right)^2 \quad \text{and} \quad q = 1-\eta.$$

For $\eta = 2$ we take the same H as for $\eta \neq 2$ but we subdivide each edge to become a path of length 3. Note that $P_0(2) = (-8)^k$ and $P_1(2) = 24^k$. The condition (4.26) becomes

$$(-1)^k + 3^{k+2} \equiv 0 \bmod p. \tag{4.35}$$

Again, we want to find sufficiently many primes p such that (4.35) can be satisfied for some integer k. This is a corollary of Lemma 4.8, taking

$$r = -9 \quad \text{and} \quad q = -1/3.$$

Hence we have the following.

Proof of Lemma 4.4. The proof is a routine application of the Chinese Remainder Theorem (similar to the proof of Lemma 4.2). We assume, for simplicity, $\eta \neq 2$ (the

case $\eta = 2$ is the same with (4.34) replaced by (4.35)). Given an instance $G = (V, E)$ of #BIS, let $n := |V|$ and L be the number of independent sets of G. Note that $L \leqslant 2^n$.

We choose n^2 primes $p_1, \ldots, p_{n^2} > 3$ such that

- for each $i \in [n^2]$, (4.34) has an integer solution to k with $p = p_i$,
- $p_i = O(n^3)$ for $i \in [n^2]$, and
- $\prod_{i=1}^{n^2} p_i > 2^n$.

By Lemma 4.8 these primes exist when $\eta \notin \{\pm 1, 0\}$, and we can find them in time polynomial in n by using an exhaustive search.

For each p_i, let $0 < k_i < p_i$ be an integer solution of (4.34) with $p = p_i$ (if k_i is a solution of (4.34) then $k_i + t(p_i - 1)$ is a solution for every $t \in \mathbb{Z}$), again we can find the k_i by using an exhaustive search. We then construct a bipartite graph G_i' as above from G, p_i and k_i. Note that G_i' has size polynomial in n since $k_i < p_i = O(n^3)$. As (4.34) is satisfied, by Lemma 4.11, we have

$$L \equiv \#\mathrm{PBIS}(G_i'; \eta) \bmod p_i.$$

We can make a query to the oracle to obtain the rational number $\#\mathrm{PBIS}(G_i'; \eta)$ and thus we can compute L mod p_i in polynomial time for each $i \in [n^2]$. By the Chinese Remainder Theorem, we can compute L in time polynomial in n. □

5. Conclusions

We conclude with a few questions and a discussion on approximating the R_2' polynomial.

Question 1. What other interesting properties are encoded by the polynomial?

Thanks to the referee for pointing out that the methods of [8] resolve the following question in the positive (the R_2 polynomial is MS_2-definable and hence one can use Theorem 32 of [8]; see also Lemma 24 of [7]). One can still ask for a more efficient algorithm that would use more specific properties of the R_2 polynomial; see [5], where such an algorithm is given for the interlace polynomial.

Question 2. Is the exact evaluation of the polynomial easy for bounded tree-width graphs?

Because of the hardness of exact evaluation of R_2', another question is whether there is a fully polynomial randomized approximation scheme (FPRAS) for $R_2'(G; \lambda, \mu)$. Results of [19] imply that there is an FPRAS for $R_2'(G; \lambda, \mu)$ when $\lambda = 1/2$ and $-1 < \mu < 0$. This follows from Theorem 4.3 and the fact that there is an FPRAS for $\#\mathrm{PBIS}(\eta)$ (defined by (4.6) in Section 4) when $0 < \eta < 1$ (this follows from [19] and the fact that $\#\mathrm{PBIS}(\eta)$ corresponds to $\beta = 1$, $\gamma = (1 + \eta)/(1 - \eta)$ and $\mu = 1$ in their parametrization).

One way of designing an FPRAS is the Markov chain Monte Carlo method. The natural sampling problem associated with R_2' is the following.

Rank Weighted Subgraphs with $\lambda, \mu \geqslant 0$, (RWS(λ, μ)).
Input: a bipartite graph $G = (U \cup W, E)$,
Output: $S \subseteq E$ with probability of $S \propto \lambda^{\mathrm{rk}_2(S)}\mu^{|S|}$.

Note that the problem of (approximately) evaluating the polynomial is self-reducible (we can remove one edge), and hence by [22] sampling is equivalent to counting.

The 'single bond flip' chain is a natural approach to sampling from RWS(λ, μ).

Definition. The *single bond flip* chain is defined as follows. Pick an edge $e \in E$ at random and let $S = X_t \oplus \{e\}$. Set $X_{t+1} = S$ with probability

$$(1/2)\min\{1, \lambda^{\mathrm{rk}_2(S)-\mathrm{rk}_2(X_t)}\mu^{|S|-|X_t|}\} \tag{5.1}$$

and $X_{t+1} = X_t$ with the remaining probability.

In each step of the single bond flip chain, we have to compute the rank of a matrix over $\mathbb{F}_2$ (corresponding to S) which differs from the current matrix (corresponding to X_t) in a single entry. One can use dynamic matrix rank problem algorithms to perform this computation in $O(n^{1.575})$ arithmetic operations per step [15].

In the initial version of this paper [16], we proved that the chain is rapidly mixing for trees. Bordewich and Kang [6] recently proved that the single bond flip chain mixes in polynomial time for graphs of constant tree-width. Unfortunately, Goldberg and Jerrum [18] recently showed that there exist bipartite graphs for which the single bond flip chain has exponential mixing time for $\lambda = 1/2$ and $\mu = 1$ (which is the most interesting setting of λ and μ). Nevertheless, there may exist interesting classes of graphs for which the chain mixes, motivating the following question.

Question 3. For which classes of bipartite graphs does the single bond flip chain mix?

References

[1] Arratia, R., Bollobás, B. and Sorkin, G. B. (2004) A two-variable interlace polynomial. *Combinatorica* **24** 567–584.

[2] Bach, E. and Shallit, J. (1996) *Algorithmic Number Theory*, Vol. 1, *Efficient Algorithms*, Foundations of Computing Series, MIT Press.

[3] Baxter, R. J. (1989) *Exactly Solved Models in Statistical Mechanics*, Academic Press. Reprint of the 1982 original.

[4] Bläser, M. and Hoffmann, C. (2008) On the complexity of the interlace polynomial. In *STACS* (S. Albers and P. Weil, eds), Vol. 1 of *LIPIcs*, Leibniz-Zentrum für Informatik, pp. 97–108.

[5] Bläser, M. and Hoffmann, C. (2011) Fast evaluation of interlace polynomials on graphs of bounded treewidth. *Algorithmica* **61** 3–35.

[6] Bordewich, M. and Kang, R. J. (2011) Rapid mixing of subset Glauber dynamics on graphs of bounded tree-width. In *ICALP (1)*, pp. 533–544.

[7] Courcelle, B. (2008) A multivariate interlace polynomial and its computation for graphs of bounded clique-width. *Electron. J. Combin.* **15** #R69.

[8] Courcelle, B., Makowsky, J. A. and Rotics, U. (2001) On the fixed parameter complexity of graph enumeration problems definable in monadic second-order logic. *Discrete Appl. Math.* **108** 23–52.

[9] Dyer, M. E., Frieze, A. M. and Jerrum, M. R. (2002) On counting independent sets in sparse graphs. *SIAM J. Comput.* **31** 1527–1541.

[10] Dyer, M. E., Goldberg, L. A., Greenhill, C. and Jerrum, M. R. (2004) The relative complexity of approximate counting problems. *Algorithmica* **38** 471–500.
[11] Dyer, M. E., Goldberg, L. A. and Jerrum, M. R. (2010) An approximation trichotomy for boolean #CSP. *Journal of Computer and System Sciences* **76** 267–277.
[12] Dyer, M. E. and Greenhill, C. (2000) On Markov chains for independent sets. *J. Algorithms* **35** 17–49.
[13] Ellis-Monaghan, J. and Merino, C. (2011) Graph polynomials and their applications I: The Tutte polynomial. *Structural Analysis of Complex Networks* (M. Dehmer, ed.), Birkhuser Boston, pp. 219–255.
[14] Ellis-Monaghan, J. and Merino, C. (2011) Graph polynomials and their applications II: Interrelations and interpretations. *Structural Analysis of Complex Networks* (M. Dehmer, ed.), Birkhuser Boston, pp. 257–292.
[15] Frandsen, G. S. and Frandsen, P. F. (2006) Dynamic matrix rank. In *Automata, Languages and Programming, Part I*, Vol. 4051 of *Lecture Notes in Computer Science*, Springer, pp. 395–406.
[16] Ge, Q. and Štefankovič, D. (2010) A graph polynomial for independent sets of bipartite graphs. In *FSTTCS*, pp. 240–250.
[17] Goldberg, L. A. and Jerrum, M. R. (2007) The complexity of ferromagnetic Ising with local fields. *Combin. Probab. Comput.* **16** 43–61.
[18] Goldberg, L. A. and Jerrum, M. R. (2010) Personal communication.
[19] Goldberg, L. A., Jerrum, M. R. and Paterson, M. (2003) The computational complexity of two-state spin systems. *Random Struct. Alg.* **23** 133–154.
[20] Jaeger, F., Vertigan, D. and Welsh, D. J. A. (1990) On the computational complexity of the Jones and Tutte polynomials. *Math. Proc. Cambridge Philos. Soc.* **108** 35–53.
[21] Jerrum, M. R. and Sinclair, A. (1993) Polynomial-time approximation algorithms for the Ising model. *SIAM J. Comput.* **22** 1087–1116.
[22] Jerrum, M. R., Valiant, L. G. and Vazirani, V. V. (1986) Random generation of combinatorial structures from a uniform distribution. *Theoret. Comput. Sci.* **43** 169–188.
[23] Luby, M. and Vigoda, E. (1999) Fast convergence of the Glauber dynamics for sampling independent sets. *Random Struct. Alg.* **15** 229–241.
[24] Makowsky, J. A. (2008) From a zoo to a zoology: Towards a general theory of graph polynomials. *Theory Comput. Syst.* **43** 542–562.
[25] Moree, P. and Stevenhagen, P. (2000) A two-variable Artin conjecture. *J. Number Theory* **85** 291–304.
[26] Moree, P. and Stevenhagen, P. (2001) Prime divisors of the Lagarias sequence. *J. Théor. Nombres Bordeaux* **13** 241–251.
[27] Provan, J. S. and Ball, M. O. (1983) The complexity of counting cuts and of computing the probability that a graph is connected. *SIAM J. Comput.* **12** 777–788.
[28] Sly, A. (2010) Computational transition at the uniqueness threshold. In *Proc. 51st Annual IEEE Symposium on Foundations of Computer Science* (*FOCS*), pp. 287–296.
[29] Stevenhagen, P. (2000) Prime densities for second order torsion sequences. Preprint.
[30] Tutte, W. T. (1947) A ring in graph theory. *Proc. Cambridge Philos. Soc.* **43** 26–40.
[31] Tutte, W. T. (1954) A contribution to the theory of chromatic polynomials. *Canadian J. Math.* **6** 80–91.
[32] Vadhan, S. P. (2001) The complexity of counting in sparse, regular, and planar graphs. *SIAM J. Comput.* **31** 398–427.
[33] Weitz, D. (2006) Counting independent sets up to the tree threshold. In *STOC'06: Proc. 38th Annual ACM Symposium on Theory of Computing*, ACM, pp. 140–149.
[34] Welsh, D. J. A. (1993) *Complexity: Knots, Colourings and Counting*, Vol. 186 of *London Mathematical Society Lecture Note Series*, Cambridge University Press.
[35] Xia, M., Zhang, P. and Zhao, W. (2007) Computational complexity of counting problems on 3-regular planar graphs. *Theoret. Comput. Sci.* **384** 111–125.