ENUMERATION AND ALGORITHMS

MARTIN LOEBL

Abstract. We introduce some basic concepts which interlace algorithms, enumeration and statistical physics.

Contents

1. Introduction

sec.intro

A graph is a pair (V, E) where V is a set of *vertices* and E is a set of unordered pairs from V, called *edges*. The notions of graph theory we will use are so natural there is no need to introduce them.

1.1. Euler's Theorem.
Perhaps the first theorem of graph theory is the Euler's theorem, and it is also about walking.

Theorem 1. *A graph $G = (V, E)$ has a closed walk containing each edge exactly once if and only if it is connected and each vertex has an even number of edges incident with it.*

Date: This edition: December 16, 2009 First edition: July 2009.

This theorem has an easy proof. Let us call a set A of edges *even* if each vertex of V is incident with an even number of edges of A. Connectivity and evenness are clearly necessary conditions for the existence of such a closed walk. Sufficiency follows from the following two lemmas.

Lemma 1.1. *Each even set of edges is a disjoint union of sets of edges of cycles.*

Lemma 1.2. *A connected set of disjoint cycles admits a closed walk which goes through each edge exactly once.*

The first lemma might be called *the greedy principle of walking*: to prove the first lemma we observe first that each non-empty even set contains a cycle; if we delete it, we again get an even set and we can continue in this way until the remaining set is empty. The proof of the second lemma is also simple: we can compose the closed walk by the walks along the disjoint cycles.

2. Even sets of edges as a kernel

We will often not distinguish a subset A of edges and its incidence vector χ_A, i.e. $0,1$-vector indexed by the edges of G, with $(\chi_A)_e = 1$ iff $e \in A$. Let $\mathcal{E}(G)$ be the set of the even subsets of edges of the graph G.

We denote by I_G the *incidence matrix* of graph G, i.e. matrix with rows indexed by $V(G)$, columns indexed by $E(G)$, and $(I_G)_{ve}$ equal to one if $v \in e$ and zero otherwise. We immediately have

Observation 2.1. *$\mathcal{E}(G)$ forms the $GF[2]$-kernel of I_G, i.e. $\mathcal{E}(G) = \{v; I_G v = 0 \text{ modulo } 2\}$.*

What is the orthogonal complement of $\mathcal{E}(G)$ in $GF[2]^{E(G)}$? It is the set $\mathcal{C}(G)$ of edge-cuts of G; a set A of edges is called *edge-cut* if there is a set U of vertices such that $A = \{e \in E; |e \cap U| = 1\}$.

3. Max-Cut, Min-Cut problems

Max-Cut and Min-Cut problems belong to the basic hard problems of computer science. Given a graph $G = (V, E)$ with a (rational) weight $w(e)$ assigned to each edge $e \in E$, the Max-Cut problem asks for the maximum value of $\sum_{e\in C} w(e)$ over all edge-cuts of G, while the Min-Cut problem asks for the minimum of the same function.

Max-Cut problem is hard (NP-complete) for non-negative edge-weights and hence both Max-Cut and Min-Cut problems are hard for general rational edge-weights. The Min-Cut problem is efficiently (polynomially) solvable for non-negative edge-weights. This has been a fundamental result of computer science, and is known as 'max-flow, min-cut algorithm'.

Still, there are some special important classes of graphs where the Max-Cut problem is efficiently solvable. One such class is the class of the planar graphs.

3.1. **Max-Cut problem for planar graphs.** A graph is called *planar* if it can be represented in the plane so that the vertices are different points, the edges are *arcs* (by arc we mean an injective continuous map of the closed interval $[0,1]$ to the plane) connecting the representations of their vertices, and disjoint with the rest of the representation. We will also say that the planar graphs have *proper planar drawing*, and a properly drawn planar graph will be called *topological planar graph*. Let G be a topological planar graph and let γ be the subset of the plane consisting of the planar representation of G. After deletion of γ, the plane is partitioned into 'islands' which are called *faces* of G. We let $F(G)$ be the set of the faces of G and we will denote by $v(G), e(G), f(G)$ the number of vertices, edges and faces of G and recall the Euler's formula: $v(G) - e(G) + f(G) = 2$.

An important concept we need is that of *dual graph* G^* of a topological graph G. It turns out convenient to define G^* as an abstract (not topological) graph. But we need to allow multiple edges and loops which is not included in the concept of the graph as a pair (V, E), where $E \subset \binom{V}{2}$.

A standard way out is to define a graph as a triple (V, E, g) where V, E are sets and g is a function from E to $\binom{V}{2} \cup V$ which gives to each edge its terminal vertices. For instance $e \in E$ is a loop iff $g(e) \in V$.

Now we can define G^* as triple $(F(G), \{e^*; e \in E(G)\}, g)$ where $g(e^*) = \{f \in F(G);\, e \text{ belongs to the boundary of } f\}$.

If G is a topological planar graph then G^* is planar. There is a natural way to properly draw G^* to the plane: represent each vertex $f \in F(G)$ as a point in the face f, and represent each edge e^* by an arc between the corresponding points, which crosses exactly once the representation of e in G and is disjoint with the rest of the representations of G and G^*.

We will say that a set A of edges of a topological planar graph is *dual even* if $\{e^*; e \in A\}$ is an even set of edges of G^*.

Observation 3.1. *The dual even subsets of edges of G are exactly the edge-cuts of G^*.*

These considerations reduce the Max-Cut problem in the class of the planar graphs to the following problem, again in the class of the planar graphs:

Maximum even subset problem. Given a graph $G = (V, E)$ with rational weights on the edges, find the maximum value of $\sum_{e \in H} w(e)$ over all even subsets H of edges.

Finally the following theorem means that the Max-Cut problem is efficiently solvable for the planar graphs.

Theorem 2. *The Maximum even subset problem is efficiently solvable for general graphs.*

4. Edwards-Anderson Ising model

The Max-Cut problem has a long history in computer science, but one of the basic applications comes from the study of the *Ising model*, a theoretical physics model of the nearest-neighbor interactions in a crystal structure.

In the Ising model, the vertices of a graph $G = (V, E)$ represent particles and the edges describe interactions between pairs of particles. The most common example is a planar square lattice where each particle interacts only with its neighbors. Often, one adds edges connecting the first and last vertex in each row and column, which represent *periodic boundary conditions* in the model. This makes the graph a *toroidal square lattice*.

Now, we assign a factor J_{ij} to each edge $\{i, j\}$; this factor describes the nature of the interaction between particles i and j. A physical state of the system is an assignment of $\sigma_i \in \{+1, -1\}$ to each vertex i. This describes the two possible spin orientations the particle can take. The *Hamiltonian* (or *energy function*) of the system is then defined as

$$H(\sigma) = -\sum_{\{i,j\}\in E} J_{ij}\sigma_i\sigma_j$$

One of the key questions we may ask about a specific system is:

"What is the lowest possible energy (the *ground state*) of the system?"

Before we seek an answer to this question, we should realize that the physical states (spin assignments) correspond exactly to the edge-cuts of the underlying graph with specified 'shores'. Let us define:

$$V_1 = \{i \in V; \sigma_i = +1\}$$
$$V_2 = \{i \in V; \sigma_i = -1\}$$

Then this partition of vertices encodes uniquely the assignment of spins to particles. The edges contained in the edge-cut $C(V_1, V_2)$ are those connecting a pair of particles with different spins, and those outside the cut connect pairs with equal spins. This allows us to rewrite the Hamiltonian in the following way:

$$H(\sigma) = \sum_{\{i,j\}\in C} J_{ij} - \sum_{\{i,j\}\in E\setminus C} J_{ij} = 2w(C) - W,$$

where $w(C) = \sum_{\{i,j\}\in C} J_{ij}$ denotes the weight of a cut, and $W = \sum_{\{i,j\}\in E} J_{ij}$ is the sum of all edge weights in the graph.

Clearly, if we find the value of MAX-CUT, we have found the maximum energy of the physical system. Similarly, MIN-CUT (the cut with minimum possible weight) corresponds to the minimum energy of the system.

The distribution of the physical states over all possible energy levels is encapsulated in the *partition function*:

$$Z(G,\beta) = \sum_\sigma e^{-\beta H(\sigma)}.$$

The variable β is changed for K/T in the Ising model, where K is a constant and T is a variable representing the temperature.

It follows from 3.1 that there is an efficient algorithm to determine the ground state energy of the Ising model on any planar graph. In fact the whole partition function may be determined efficiently for planar graphs, and a principal ingredient is the following concept of 'enumeration duality'.

5. An enumeration duality

It turns out that the Ising partition function for a graph G may be expressed in terms of the generating function of the even sets of the same graph G. This is the seminal theorem of Van der Waerden whose proof is so simple that we include it here. We will use the following standard notations: $\sinh(x) = 1/2(e^x - e^{-x})$, $\cosh(x) = 1/2(e^x + e^{-x})$, $\tanh(x) = \frac{\sinh(x)}{\cosh(x)}$.

Theorem 3. *Let $G = (V,E)$ be a graph with edge weights $J_{ij}, ij \in E$. Then*

$$Z(G,\beta) = 2^{|V|} \prod_{ij\in E} \cosh(\beta J_{ij}) \mathcal{E}(G,x)|_{x^{J_{ij}} := \tanh(\beta J_{ij})}.$$

Proof. We have

$$Z(G,\beta) = \sum_\sigma e^{\beta \sum_{ij} J_{ij}\sigma_i\sigma_j} = \sum_\sigma \prod_{ij\in E} (\cosh(\beta J_{ij}) + \sigma_i\sigma_j \sinh(\beta J_{ij})) =$$

$$\prod_{ij\in E} \cosh(\beta J_{ij}) \sum_\sigma \prod_{ij\in E} (1 + \sigma_i\sigma_j \tanh(\beta J_{ij})) =$$

$$= \prod_{ij\in E} \cosh(\beta J_{ij}) \sum_\sigma \sum_{A\subset E} \prod_{ij\in E} \sigma_i\sigma_j \tanh(\beta J_{ij}) =$$

$$= \prod_{ij\in E} \cosh(\beta J_{ij}) \sum_{A\subset E} (U(A) \prod_{ij\in A} \tanh(\beta J_{ij})),$$

where

$$U(A) = \sum_\sigma \prod_{ij\in A} \sigma_i\sigma_j.$$

The proof is complete when we notice that $U(A) = 2^{|V|}$ if A is even and $U(A) = 0$ otherwise. $\square$

We saw above that $Z(G, \beta)$ may be looked at as the generating function of the edge-cuts with the specified shores. The theorem of Van der Waerden expresses it in terms of the generating function $\mathcal{E}(G, x)$ of the even sets of edges.

We can also consider the honest *generating function of edge-cuts* defined by

$$\mathcal{C}(G, x) = \sum_{cutC} x^{w(C)},$$

where the sum is over all edge-cuts of G and $w(C) = \sum_{e \in C} w(e)$.

It turns out that $\mathcal{C}(G, x)$ may also be expressed in terms of $\mathcal{E}(G, x)$. This is a consequence of another seminal theorem, of MacWilliams which we explain now.

Let $C \subset GF[2]^n$ be a *binary code*, i.e. a subspace over $GF[2]$. Let $A_i(C)$ denote the number of vectors of C with exactly i occurrences of 1. The *weight enumerator* of C is defined as

$$A_C(y) = \sum_{i \geq 0} A_i(C) y^i.$$

let us denote by C^* the *dual code*, i.e. the orthogonal complement of C. MacWilliam's theorem reads as follows:

Theorem 4.
$$A_{C^*}(y) = \frac{1}{|C|}(1+y)^n A_C(\frac{1-y}{1+y}).$$

We saw before that the set of the edge-cuts and the set of the even sets of edges form dual binary codes, hence MacWilliams' theorem applies.

This theorem is true more generally for linear codes over finite field $GF[q]$; hence it applies to the kernel and the image of the incidence matrix of a graph, viewed over $GF[q]$. This is related to the extensively studied field of *nowhere-zero flows*.

6. Inclusion and Exclusion

Let us start with the introduction of a paper of Hassler Whitney, which appeared in Annals of Mathematics in August 1932:

"Suppose we have a finite set of objects (for instance books on a table), each of which either has or has not a certain given property A (say of being red). Let n be the total number of objects, $n(A)$ the number with the property A, and $n(\bar{A})$ the number without the property A. Then obviously $n(\bar{A}) = n - n(A)$. Similarly, if $n(AB)$ denote the number with both properties A and B, nad $n(\bar{A}\bar{B})$ the number with neither property, then $n(\bar{A}\bar{B}) = n - n(A) - n(B) + n(AB)$, which is easily seen to be true.

The extension of these formulas to the general case where any number of properties are considered is quite simple, and is well known to logicians. It should be better known to mathematicians also; we give in this paper several applications which show its usefulness."

Indeed, we all know it, under the name 'inclusion-exclusion principle':

if $A_1, ..., A_n$ are finite sets, and if we let $\bigcap(A_i; i \in J) = A_J$ then

$$\left|\bigcup(A_i; i = 1, ..., n)\right| = \sum_{k=1}^{n}(-1)^{k-1} \sum_{J \in \binom{n}{k}} |A_J|.$$

7. The chromatic polynomial and the Tutte polynomial

In the before-mentioned paper, Whitney mentions a formula for the number of ways of coloring a graph as one of the main applications of PIE. Let us again follow the article of Whitney for a while:

Suppose we have a fixed number z of colors at our disposal. Any way of assigning one of these colors to each vertex of the graph in such a way that any two vertices which are joined by an arc are of different colors, will be called admissible coloring, using z or fewer colors. We wish to find the number $M(z)$ of admissible colorings, using z or fewer colors. ... We shall deduce a formula for $M(z)$ due to Birkhoff.

If there are V vertices in the graph G, then there are $n = z^V$ possible colorings, formed by giving each vertex in succession any one of z colors. Let R be this set of colorings. Let A_{ab} denote those colorings with the property that a and b are of the same color, etc. Then the number of admissible colorings is

$$\begin{aligned} M(z) = n - [n(A_{ab}) + n(A_{bd}) + ... + n(A_{cf})] \\ +[n(A_{ab}A_{bd}) + ...] - ... \\ +(-1)^E n(A_{ab}A_{bd}...A_{cf}). \end{aligned}$$

With each property A_{ab} is associated an arc ab of G. In the logical expansion, there is a term corresponding to every possible combination of the properties A_{pq}; with this combination we associate the corresponding edges, forming a subgraph H of G. In particular, the first term corresponds to the subgraph containing no edges, and the last term corresponds to the whole of G. We let H contain all the vertices of G.

Let us evaluate a typical term $n(A_{ab}A_{ad}...A_{ce})$. This is the number of ways of coloring G in z or fewer colors in such a way that a and b are of the same color, a and d are of the same color, ..., c and e are of the same color. In the corresponding subgraph H, any two vertices that are joined by an edge must be of the same color, and thus all the vertices in a single connected piece in H are of the same color. If there are p connected pieces in H, the value of this term is therefore z^p. If there are s edges in H, the sign of the term is $(-1)^s$. Thus

$$(-1)^s n(A_{ab}A_{bd}...A_{cf}) = (-1)^s z^p.$$

If there are (p, s) (this is Birkhoff's symbol) subgraphs of s edges in p connected pieces, the corresponding terms contribute to $M(z)$ an amount $(-1)^s(p, s)z^p$. Therefore, summing over all values of p and s, we find the polynomial in z:

$$M(z) = \sum_{p,s}(-1)^s(p, s)z^p.$$

This function is the well-known *chromatic polynomial*. The proper colorings of graphs appeared perhaps first with the famous Four-Color-Conjecture, which is now a theorem, even though proved only with a help of computers: Is it true that each planar graph has an admissible coloring by four colors?

A graph $G = (V, E)$ is *connected* if it has a path between any pair of vertices. If a graph is not connected then its maximum connected subgraphs are called *connected components*. If $G = (V, E)$ is a graph and $A \subset E$ then let $C(A)$ denote the set of the connected components of graph (V, A) and $c(A) = |C(A)|$ denotes the number of connected components (pieces) of (V, A).

Let $G = (V, E)$ be a graph. For $A \subset E$ let $r(A) = |V| - c(A)$. Then we can write

$$M(z) = z^{c(E)}(-1)^{r(E)} \sum_{A\subset E}(-z)^{r(E)-r(A)}(-1)^{|A|-r(A)}.$$

This leads directly to Whitney rank generating function $R(G, u, v)$ defined by

$$R(G, u, v) = \sum_{A\subset E} u^{r(E)-r(A)}v^{|A|-r(A)}.$$

We start considering the *Tutte polynomial*; it has been defined by Tutte and it may be expressed as a minor modification of the Whitney rank generating function.

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

$T(G, x, y)$ is called the *Tutte polynomial* of graph G.

Note that for any connected graph G, $T(G, 1, 1)$ counts the number of spanning trees of G: indeed, the only terms that count are those for which $r(A) = r(E) = |A|$. These are exactly the spanning trees of G.

The Tutte polynomial is directly related to the partition function of another basic model of statistical physics, the *Potts model*. Potts specialises to Ising.

7.1. **The dichromate and the Potts partition function.** The following function called *dichromate* is extensively studied in combinatorics. It is equivalent to the Tutte polynomial.

$$B(G,a,b) = \sum_{A \subset E} a^{|A|} b^{c(A)}.$$

Definition 7.1. Let $G = (V,E)$ be a graph, $k \geq 1$ integer and J_e a weight (coupling constant) associated with edge $e \in E$. The *Potts model partition function* is defined as

$$P^k(G, J_e) = \sum_s e^{E(P^k)(s)},$$

where the sum is over all functions (states) s from V to $\{1, \ldots, k\}$ and

$$E(P^k)(s) = \sum_{\{i,j\} \in E} J_{ij} \delta(s(i), s(j)).$$

We may write

$$P^k(G, J_e) = \sum_s \prod_{\{i,j\} \in E} (1 + v_{ij} \delta(s(i), s(j))) = \sum_{A \subset E} k^{c(A)} \prod_{\{i,j\} \in A} v_{ij},$$

where $v_{ij} = e^{J_{ij}} - 1$. The RHS is sometimes called *multivariate Tutte polynomial*; If all J_{ij} are the same we get an expression of the Potts partition function in the form of the dichromate:

$$P^k(G,x) = \sum_s \prod_{\{i,j\} \in E} e^{x\delta(s(i),s(j))} = \sum_{A \subset E} k^{c(A)} (e^x - 1)^{|A|} = B(G, e^x - 1, k).$$

7.2. **The q-chromatic function and the q-dichromate.** Here we study the following *q-chromatic function on graphs*:

Definition 7.2. Let $G = (V,E)$ be a graph and n a positive integer. Let $V = \{1, \ldots, k\}$ and let $V(G,n)$ denote the set of all vectors $(v_1, \ldots, v_k)$ such that $0 \leq v_i \leq n-1$ for each $i \leq k$ and $v_i \neq v_j$ whenever $\{i,j\}$ is an edge of G. We define the q-chromatic function by:

$$M_q(G,n) = \sum_{(v_1 \ldots v_k) \in V(G,n)} q^{\sum_i v_i}.$$

Note that $M_q(G,n)|_{q=1}$ is the classic chromatic polynomial of G.

An example.

We first recall some notation:

For $n > 0$ let $(n)_1 = n$ and for $q \neq 1$ let $(n)_q = \frac{q^n - 1}{q-1}$ denote a *quantum integer*. We let $(n)!_q = \prod_{i=1}^n (i)_q$ and for $0 \leq k \leq n$ we define the *quantum binomial coefficients* by

$$\binom{n}{k}_q = \frac{(n)!_q}{(k)!_q (n-k)!_q}.$$

A simple quantum binomial formula leads to a well-known formula for the summation of the products of distinct powers. This gives the q-chromatic function for the complete graph.

Observation 7.3.

$$M_q(K_k, n) = k! \binom{n}{k}_q q^{k(k-1)/2}.$$

Let $G = (V, E)$ be a graph and $A \subset E$ with $C(A)$ denoting the set of the connected components of graph (V, A) and $c(A) = |C(A)|$. If $W \in C(A)$ then let $|W|$ denote the number of vertices of W. A standard PIE argument gives the following expression for the q-chromatic function, which enables to extend it from non-negative n to the reals.

Theorem 5.

$$M_q(G, n) = \sum_{A \subset E} (-1)^{|A|} \prod_{W \in C(A)} (n)_{q^{|W|}}.$$

The formula of Theorem 5 leads naturally to a definition of *q-dichromate.*

Definition 7.4. We let

$$B_q(G, x, y) = \sum_{A \subset E} x^{|A|} \prod_{W \in C(A)} (y)_{q^{|W|}}.$$

Note that $B_{q=1}(G, x, y) = B(G, x, y)$ and by Theorem 5, $M_q(G, n) = B_q(G, -1, n)$.

What happens if we replace $B(G, e^x - 1, k)$ by $B_q(G, e^x - 1, k)$? It turns out that this introduces an additional external field to the Potts model.

Theorem 6.

$$\sum_{A \subset E} \prod_{W \in C(A)} (k)_{q^{|W|}} \prod_{\{i,j\} \in A} v_{ij} = \sum_s q^{\sum_{v \in V} s(v)} e^{E(P^k)(s)},$$

where $v_{ij} = e^{J_{ij}} - 1$.

7.3. **Multivariate generalisations.** Let $x_1, x_2, \dots$ be commuting indeterminates and let $G = (V, E)$ be a graph. The q-chromatic function restricted to non-negative integer y is the principal specialization of X_G, the *symmetric function generalisation of the chromatic polynomial.* This has been defined by Stanley as follows:

Definition 7.5.

$$X_G = \sum_f \prod_{v \in V} x_{f(v)},$$

where the sum ranges over all proper colorings of G by $\{1, 2, \dots\}$.

Therefore $M_q(G, n) = X_G(x_i = q^i (0 \le i \le n-1), x_i = 0 (i \ge n))$.

Further Stanley defines *symmetric function generalisation of the bad colouring polynomial*:

Definition 7.6.

$$XB_G(t, x_1, \dots) = \sum_f (1+t)^{b(f)} \prod_{v \in V} x_{f(v)},$$

where the sum ranges over ALL colorings of G by $\{1, 2, \dots\}$ and $b(f)$ denotes the number of monochromatic edges of f.

Noble and Welsh define the *U-polynomial* (see Definition 7.7) and show that it is equivalent to XB_G. Sarmiento proved that the polychromate defined by Brylawski is also equivalent to the U-polynomial.

Definition 7.7.

$$U_G(z, x_1 \dots) = \sum_{S \subset E(G)} x(\tau_S)(z-1)^{|S|-r(S)},$$

where $\tau_S = (n_1 \geq n_2 \geq \dots n_k)$ is the partition of $|V|$ determined by the connected components of S, $x(\tau_S) = x_{n_1} \dots x_{n_k}$ and $r(S) = |V| - c(S)$.

The motivation for the work of Noble and Welsh is a series of papers by Chmutov, Duzhin and Lando. It turns out that the U-polynomial evaluated at $z = 0$ and applied to the intersection graphs of chord diagrams satisfies the $4T-$relation of the *weight systems*. Hence the same is true for $M_q(G, z)$ for each positive integer z since it is an evaluation of $U_G(0, x_1 \dots)$:

Observation 7.8. *Let z be a positive integer. Then*

$$M_q(G, z) = (-1)^{|V|} U_G(0, x_1 \dots)|_{x_i := (-1)(q^{i(z-1)} + \dots + 1)}.$$

Weight systems form a basic stone in the combinatorial study of the quantum knot invariants.

On the other hand, it seems plausible that the q-dichromate determines the U-polynomial. If true, q-dichromate provides a compact representation of the multivariate generalisations of the Tutte polynomial mentioned above.

8. The Zeta function of a graph

In this section we discuss the theorem of Bass, and the MacMahon Master theorem.

Let $G = (V, E)$ be a graph. If $e \in E$ then we let a_e denote an orientation of e (arbitrary but fixed), and a_e^{-1} the reversed directed edge to a_e. A circular sequence $p = v_1, a_1, v_2, a_2, ..., a_n, v_{n+1}$ and $v_{n+1} = v_1$ is called a *prime reduced cycle* if the following conditions are satisfied: $a_i \in \{a_e, a_e^{-1} : e \in E\}$, $a_i \neq a_{i+1}^{-1}$ and $(a_1, ..., a_n) \neq Z^m$ for some sequence Z and $m > 1$.

Definition 8.1. Let $G = (V, E)$ be a graph. The Ihara-Selberg function of G is

$$I(u) = \prod_\gamma (1 - u^{|\gamma|})$$

where the product is defined by

$$\prod_{\gamma}(1-u^{|\gamma|}) = \sum_{\mathcal{G}}(-1)^{|\mathcal{G}|}u^{\sum_{\gamma\in\mathcal{G}}|\gamma|},$$

and the sum is over all finite sets $\mathcal{G}$ of the prime reduced cycles. The zeta function of G is

$$Z(u) = I(u)^{-1}.$$

The theorem of Bass reads as follows:

Theorem 7. *(Bass' theorem) For any graph G*

$$I(u) = \det(I - uT),$$

where T is the matrix of transitions between directed edges defined as follows: Let $a, a' \in \{a_e, a_e^{-1} : e \in E\}$. If the terminal vertex of a is the initial vertex of a' and $a' \neq a^{-1}$ then $T_{a,a'} = 1$, otherwise $T_{a,a'} = 0$.

Next we write down the MacMahon Master theorem.

Theorem 8. *(MacMahon Master theorem) Let $A = (a_{ij})$ be an $n \times n$ matrix, and let $x = (x_1, \cdots, x_n)$ be a vector of commuting variables. The coefficient of $x_1^{m_1} \cdots x_n^{m_n}$ in*

$$\prod_{i=1}^{n}(\sum_{j=1}^{n} a_{ij}x_j)^{m_i}$$

is equal to the coefficient of $x_1^{m_1} \cdots x_n^{m_n}$ in the expansion of $[\det(I - xA)]^{-1}$.

We include the proofs of these theorems based on the theory of Lyndon words. Let X be a non-empty linearly ordered set, and consider the set X^* of all finite words from X. Let $<$ denote the lexicographic ordering on X^* derived from the linear ordering on X: for $u \neq v$ we say that $u < v$ if $v = uz$ for some $z \in X^*$, or $u = ras, v = rbt$ with $a < b$ and $r, s, t \in X^*$. We consider the set X^* of all words from X equipped with the binary operation of concatenation:

$$(a_1, \ldots, a_n)(b_1, \ldots, b_m) = (a_1, \ldots, a_n, b_1, \ldots, b_m).$$

A *Lyndon word* is a nonempty word of X^* that is prime (i.e., it cannot be written as a power of a shorter word), and minimal among its cyclic rearrangements (for example, 221 is not a Lyndon word since $221 > 122$. Let $\mathcal{L}$ denote the set of all Lyndon words.

Observation 8.2. *A non-empty word w is Lyndon if and only if w is smaller than any of its proper right factors if and only if $w \in X$ or $w = lm$ with $l, m \in \mathcal{L}$ and $l < m$.*

The following theorem is called Lyndon's factorization theorem.

Theorem 9. *Each nonempty word $l \in X^*$ can be uniquely written as a nonincreasing concatenation of Lyndon words: $l = l_1 l_2 \cdots l_n$, $l_k \in \mathcal{L}$, $l_1 \geq l_2 \geq \cdots \geq l_n$.*

Proof. To prove the theorem, we simply take a factorization $l = l_1 l_2 \cdots l_n$ into Lyndon words (a factorization like that clearly exists since each element of X is a Lyndon word) such that n is as small as possible. The Lyndon words in this factorization must be nonincreasing by Observation 8.2. The observation also proves the uniqueness.

□

Next we consider formal power series with integer coefficients, and with variables in X, which are not commuting. It is convenient to use the symbol X^* to denote $\sum_{l \in X^*} l$. As an exercise in this notation (we denote by X_r^* the set of the reversed words of X^*) prove that the Lyndon factorization theorem is the same as

$$\prod_{l \in \mathcal{L}} (1 - l)^{-1} = X_r^* = X^* = (1 - \sum_{z \in X} z)^{-1},$$

where the indices in the product appear in the increasing order.

We get Amitsur's identity as a useful corollary:

Proposition 8.3. *Let X be the set of matrices $A_1, \ldots, A_k$, linearly ordered by their indices. Then*

$$\det(I - (A_1 + \cdots + A_k)) = \prod_{l \in \mathcal{L}} \det(I - l).$$

Proof. We can write as above

$$\prod_{l \in \mathcal{L}} (I - l)^{-1} = (I - (\sum_{z \in X} z))^{-1}.$$

Now we take the inverse of this identity, and take the determinant of both sides. This finishes the proof. □

Let $\mathcal{B}$ be an $X \times X$ matrix whose entries are commuting variables. We denote the $ij-$entry of $\mathcal{B}$ by $b(i,j)$. We can think of $b(i,j)$ as the weight of the *transition* between the elements i, j of X.

Definition 8.4. Let $w = x_1 x_2 \cdots x_m$ be a nonempty word of X^*. We define

$$\beta_{circ}(w) = b(x_1, x_2) b(x_2, x_3) \cdots b(x_{m-1}, x_m) b(x_m, x_1),$$

and $\beta_{circ}(w) = 1$ if w is empty. Let $w = l_1 l_2 \cdots l_n$ be the expression of w as the nonincreasing concatenation of Lyndon words. We further define

$$\beta_{dec}(w) = \beta_{circ}(l_1) \beta_{circ}(l_2) \cdots \beta_{circ}(l_n).$$

Finally, when the m letters of w are written in the *nondecreasing order*, we get the word $w' = x'_1 x'_2 \cdots x'_m$. We let

$$\beta_{vert}(w) = b(x'_1, x_1) b(x'_2, x_2) \cdots b(x'_m, x_m).$$

We also let $\beta_{dec}(w) = \beta_{vert}(l) = 1$ if w is empty.

The following elementary observation is an exercise in the use of these new notions; it will be useful.

Observation 8.5. *Let $w \in X^*$ and let $w = l_1 \cdots l_n$ be the decomposition into a nonincreasing sequence of Lyndon words. Further, let $w = d_1 \cdots d_r$ be the decreasing factorization, where each new factor starts always when a letter smaller than or equal to each letter to its left appears. Then each Lyndon word l_i is a concatenation of factors d_j. Moreover*

$$\beta_{dec}(w) = \beta_{circ}(l_1)\beta_{circ}(l_2)\cdots\beta_{circ}(l_n) = \beta_{circ}(d_1)\beta_{circ}(d_2)\cdots\beta_{circ}(d_r).$$

The following theorem summarizes the relations among the notions we introduced. Both the theorem of Bass and the MacMahon Master theorem are straightforward consequences.

Theorem 10. *The following properties hold.*

$$\prod_{l\in\mathcal{L}}(1-\beta_{circ}(l))^{-1} = \sum_{w\in X^*}\beta_{dec}(w) \tag{1}$$

$$\sum_{w\in X^*}\beta_{dec}(w) = \sum_{w\in X^*}\beta_{vert}(w) \tag{2}$$

$$\sum_{w\in X^*}\beta_{vert}(w) = (\det(I-\mathcal{B}))^{-1} \tag{3}$$

$$\prod_{l\in\mathcal{L}}(1-\beta_{circ}(l)) = \det(I-\mathcal{B}) \tag{4}$$

Proof of the MacMahon Master theorem and Bass's theorem. The MacMahon Master theorem follows from statement (3) of Theorem 10. Bass's theorem is the statement (4) of Theorem 10 for X equal to the orientations of the edges, and $b(e,e') = u$ if e is a successor of e' and e is not the reversed e'.

Proof. (of Theorem 10) First note that (1),(2) and (4) imply (3). Next let us associate, with each Lyndon word l, a variable denoted by $[l]$. We assume that these variables are distinct and commute with each other. Let $\beta([l]) = \beta_{circ}(l)$. We have

$$\prod_{l\in\mathcal{L}}(1-\beta_{circ}(l))^{-1} = \prod_{l\in\mathcal{L}}(1-\beta([l]))^{-1} = \sum_{[l_{i_1}],\cdots,[l_{i_n}]}\beta([l_{i_1}])\beta([l_{i_2}])\cdots\beta([l_{i_n}]),$$

where the sum is over all the commuting monomials $[l_{i_1}],\cdots,[l_{i_n}]$, or equivalently over the nonincreasing collections $l_{i_1} \geq \cdots \geq l_{i_n}$ of Lyndon words. By Theorem 9, this equals

$$\sum_{w\in X^*}\beta_{dec}(w).$$

This proves (1).
In order to prove (2), we construct a bijection f of X^* onto itself so that for each w, $f(w)$ is a rearrangement of w and $\beta_{dec}(w) = \beta_{vert}(f(w))$. The construction goes as follows: Let $w \in X^*$ and let $w = l_1 \cdots l_n$ be the decomposition into the nonincreasing sequence of Lyndon words, and let $w = d_1 \cdots d_r$ be the decreasing factorization of w (see Observation 8.5). We define a set S of ordered pairs as follows: for each $1 \leq i \leq r$, if $d_i = i_1 \cdots i_p$ then we put the pairs $(i_1, i_2), \cdots, (i_{p-1}, i_p), (i_p, i_1)$ into S. We define $f(w)$ to be the word consisting of the second elements of each pair of S, written according to the nondecreasing lexicographic order of S. The properties of f follow from Observation 8.5.
Finally we show that (4) follows from Amitsur's identity (Theorem 8.3). We consider the lexicographic order on the indices of $\mathcal{B}$ (i.e. on the elements of $X \times X$). If ij is the m-th pair then let A_m be the matrix whose entries are all zero except $(A_m)_{ij} = b(i,j)$. Then $A_1 + \cdots + A_{|X|^2} = \mathcal{B}$. Consider a word $l = (i_1, j_1), \cdots, (i_p, j_p)$ in the alphabet X^2 and let $A_l = \prod_{s=1}^{p} A_{(i_s, j_s)}$. If $j_1 = i_2, j_2 = i_3, \cdots, j_{p-1} = i_p$ then A_l is the matrix whose elements are all zero except $(A_l)_{i_1 j_p} = b(i_1, i_2) b(i_2, i_3) \cdots b(i_p, j_p)$. In all other cases A_l is the zero matrix. Hence, if $j_p = i_1$ we have $\det(I - A_l) = 1 - b(i_1, i_2) b(i_2, i_3) \cdots b(i_p, i_1)$, and in all the other cases we have $\det(I - A_l) = 1$. It means that the infinite product in Amitsur's identity may be restricted to the Lyndon words $l = (i_1, j_1), \cdots, (i_p, j_p)$ satisfying $j_1 = i_2, j_2 = i_3, \cdots, j_{p-1} = i_p, j_p = i_1$. But these are in bijection with the Lyndon words $i_1 \cdots i_p$ in the alphabet X.

$\square$

We conclude this section by a reformulation of the MacMahon Master theorem in terms of flows. A *natural flow* f on a digraph G is a function $f : E \longrightarrow \mathbb{N}$ on the edges of G that satisfies Kirchhoff's current law

$$\sum_{e \text{ begins at } v} f(e) = \sum_{e \text{ ends at } v} f(e)$$

at all vertices v of G. Let us set

$$f(v) = \sum_{e \text{ begins at } v} f(e).$$

Let $\mathcal{F}(G)$ denote the *set of all natural flows* of a digraph G. If β is a weight function on the set of edges of G and f is a flow on G, then

- the *weight* $\beta(f)$ of f is given by $\beta(f) = \prod_e \beta(e)^{f(e)}$, where $\beta(e)$ is the weight of the edge e.
- The *multiplicity* at a vertex v with outgoing edges $e_1, e_2, \cdots$ is given by $\text{mult}_v(f) = \binom{f(e_1)+f(e_2)+\cdots}{f(e_1), f(e_2), \cdots}$, and the *multiplicity* of f is given by $\text{mult}(f) = \prod_v \text{mult}_v(f)$.
- If E' is a subset of edges then we let $f(E') = \sum_{e \in E'} f(e)$.

Theorem 11. *If G is a digraph with the edge-weights given by matrix $\mathcal{B}$, then*

$$\frac{1}{\det(I-\mathcal{B})} = \sum_{f \in \mathcal{F}(G)} \beta(f)\,\mathrm{mult}(f).$$

Proof. This is another reformulation of statement (3) of Theorem 10: we observe that $\beta_{vert}(w) = \beta(f)$ for a natural flow f and $\mathrm{mult}(f)$ elements $w \in X^*$. □

For $r = 1$, the above corollary states that

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$$

where $x = b_{11}$. Thus, Corollary 11 is a version of the geometric series summation.

9. Pfaffians, dimers, permanents

Let $G = (V, E)$ be a graph and let M, N be two perfect matchings of G. We recall that $M \subset E$ is a matching if $e \cap e' = \emptyset$ for each pair e, e' of edges of M, and a matching is perfect if its elements contain all the vertices of graph G. A cycle is alternating with respect to a perfect matching M if it contains alternately edges of M and out of M; each alternating cycle thus has an even length. We further recall that Δ denotes the symmetric difference, $X\Delta Y = (X \setminus Y) \cup (Y \setminus X)$. If m and N are two perfect matchings then $M\Delta N$ consists of vertex disjoint alternating cycles.
Let C be a cycle of G of an even length and let D be an orientation of G. C is said to be *clockwise even* in D if it has an even number of edges directed in D in agreement with a chosen direction of traversal. Otherwise C is called *clockwise odd*.

Definition 9.1. Let G be a graph with a weight function w on the edges. Let D be an orientation of G. Let M be a perfect matching of G. For each perfect matching P of G let $\mathrm{sign}(D, M\Delta P) = (-1)^z$ where z is the number of clockwise even alternating cycles of $M\Delta P$. Moreover let

$$\mathcal{P}(D, M) = \sum_{P \text{ perfect matching}} \mathrm{sgn}(D, M\Delta P) x^{w(P)}.$$

Let $G = (V, E)$ be a graph with $2n$ vertices and D an orientation of G. Denote by $A(D)$ the skew-symmetric matrix with the rows and the columns indexed by V, where $a_{uv} = x^{w(u,v)}$ in case (u, v) is an arc of D, $a_{u,v} = -x^{w(u,v)}$ in case (v, u) is an arc of D, and $a_{u,v} = 0$ otherwise.

Definition 9.2. The *Pfaffian* of $A(D)$ is defined as

$$\mathrm{Pf}(A(D)) = \sum_P s^*(P) a_{i_1 j_1} \cdots a_{i_n j_n},$$

where $P = \{\{i_1 j_1\}, \cdots, \{i_n j_n\}\}$ is a partition of the set $\{1, \cdots, 2n\}$ into pairs, $i_k < j_k$ for $k = 1, \cdots, n$, and $s^*(P)$ equals the sign of the permutation $i_1 j_1 \cdots i_n j_n$ of $12 \cdots (2n)$. Hence, each nonzero term of the expansion of the Pfaffian equals $x^{w(P)}$ or $-x^{w(P)}$ where P is a perfect matching of G. If $s(D,P)$ denotes the sign of the term $x^{w(P)}$ in the expansion, we may write

$$\mathrm{Pf}(A(D)) = \sum_P s(D,P) x^{w(P)}.$$

The following theorem was proved by Kasteleyn.

Theorem 12. *Let G be a graph and D an orientation of G. Let P, M be two perfect matchings of G. Then*

$$s(D,P) = s(D,M)\mathrm{sign}(D, M\Delta P).$$

Corollary 9.3.

$$\mathrm{Pf}(A(D)) = s(D,M)\mathcal{P}(D,M).$$

The relevance of the Pfaffians in our context lies in the fact that the Pfaffian is a determinant-type function. The determinants are invariant under elementary row/column operations and these can be used in the Gaussian elimination to calculate a determinant. The Pfaffian may be computed efficiently by a variant of Gaussian elimination. Let A be an antisymmetric $2n \times 2n$ matrix. A *cross* of the matrix A is the union of a row and a column of the same index: the k-th cross is the following set of elements:

$$A_k = \{a_{ik}; 1 \le i \le 2n\} \cup \{a_{kj}; 1 \le j \le 2n\}.$$

Multiplying a cross A_k by a scalar α means multliplying each element of A_k by α.
Swapping crosses A_k and A_l means exchanging both the respective rows and columns. Another way of regarding the swap operation is that it exchanges the values of k and l in both of the index positions. The resulting matrix B is antisymmetric again;
Adding cross A_k to cross A_l means adding first the k-th row to the l-th one, and then adding the respective columns. The matrix remains antisymmetric.

These operations may be used to transform matrix A by at most $O(n^2)$ cross operations into a form where the Pfaffian can be determined trivially. Moreover, for graphs with some restrictive properties, e.g. for graphs with bounded genus, there are more efficient ways to perform the elimination. Apart of the Gaussian elimination, we also have the following classical theorem of Cayley.

Theorem 13.

$$(\mathrm{Pf}(A(D)))^2 = det(A(D)).$$

Kasteleyn introduced the following seminal notion:

Definition 9.4. A graph G is called Pfaffian if it has a *Pfaffian orientation*, i.e., an orientation such that all alternating cycles with respect to an arbitrary fixed perfect matching M of G are clockwise odd.

If G has a Pfaffian orientation D, then by Theorem 12 the signs $s(D, P)$ are all equal and $\mathcal{P}(G, x)$ is equal to $\mathrm{Pf}(A(D))$ up to a sign. Kasteleyn proved that each planar graph has a Pfaffian orientation.

Theorem 14. *Every topological planar graph has a Pfaffian orientation in which all inner faces are clockwise odd.*

Proof. Let G be a topological planar graph, and let M be a perfect matching in it. Without loss of generality we assume that G is 2-connected. Each face is then bounded by a cycle. Starting with an arbitrary inner face, we can gradually construct an orientation D such that in D, each inner face is clockwise odd. Next we observe, e.g. by induction on the number of faces, that this orientation D satisfies: A cycle is clockwise odd if and only if it encircles an even number of vertices. However, each alternating cycle with a perfect matching in the complement must encircle an even number of vertices, and hence it is clockwise odd. □

As a consequence we obtain the following theorem of Kasteleyn.

Theorem 15. *Each planar graph has an orientation D so that*

$$\mathcal{P}(G, x) = \mathrm{Pf}(A(D)).$$

Kasteleyn stated that for a graph of genus g, $\mathcal{P}(G, x)$ is a linear combination of 4^g Pfaffians. This was proved by Galluccio, Loebl and independently by Tesler. There were earlier partial results towards the proof by Regge and Zecchina. Tesler extended the result to the non-orientable surfaces. Galluccio and Loebl in fact proved the following compact formula.

Theorem 16. *If G is a graph of genus g then it has 4^g orientations $D_1, \cdots, D_{4^g}$ so that*

$$\mathcal{P}(G, x) = 2^{-g} \sum_{i=1}^{4^g} \mathrm{sign}(D_i) Pf(A(D_i), x),$$

for well-defined $\mathrm{sign}(D_i) \in \{1, -1\}$.

Such a linear combination repair of a non-zero genus complication is a basic technique used both by mathematicians and physicists. The earliest work I have seen it in is by Kac and Ward; we will get to it in the next section. The next section also contains a theorem analogous to

Theorem 16; there we will include the proof. Theorem 16 has attractive algorithmic consequences.

Corollary 9.5. *The Ising partition function $Z(G, \beta)$ can be determined efficiently for the topological graphs on an arbitrary surface of bounded genus. Also, the whole density function of the weighted edge-cuts, or weighted perfect matchings, may be computed efficiently for such graphs. Another well-known problem which is efficiently solvable for these graphs by the method of Theorem 16 is the exact matching problem: Given a positive integer k, a graph G and let the edges of G be colored by blue and red. It should be decided if there is a perfect matching with exactly k red edges.*
The efficiency is in the following sence: if we have integer weights, then the complexity is polynomial in the sum of the absolute values of the edge-weights.

We remark that a stronger notion of efficiency, where the complexity needs to be polynomial in the size of the graph plus the maximum of the logarithms of the edge-weights, is more customary. The existence of a polynomial algorithm in this sence is still open.
Curiously, there is no other polynomial method known to solve the max-cut problem alone even for the graphs on the torus. The method of Theorem 16 led to a useful implementation by Vondrák.

Question 1. Is there an efficient combinatorial algorithm for the toroidal max-cut problem?

A lot of attention was given to the problem of characterizing graphs which admit a Pfaffian orientation. The problem of recognizing the Pfaffian bipartite graphs goes implicitly back to 1913, when Pólya asked for a characterization of convertible matrices (this is the 'Pólya scheme'). A matrix A is *convertible* if one can change some signs of its entries to obtain a matrix B such that $\mathrm{per}(A) = \det(B)$. A polynomial-time algorithm to recognize the Pfaffian bipartite graphs (this problem is equivalent to the Pólya problem described above) has been obtained by McCuaig, Robertson, Seymour and Thomas. For the recognition of the Pfaffian graphs embeddable on an arbitrary 2-dimensional surface, there is a polynomial algorithm by Galluccio and Loebl (using Theorem 16). Theorem 16 can also be used in a straightforward way to complete the Pólya scheme.

Corollary 9.6. *For each matrix A there are matrices B_i, $i = 1, \cdots, 4^g$, obtained from A by changing signs of some entries, so that $\mathrm{per}(A)$ is an alternating sum of the $\det(B_i)$'s. The parameter g is the genus of the bipartite graph determined by the non-zero entries of A.*

Several researchers (Hammersley, Heilmann, Lieb, Godsil, Gutman) noticed that $\mathrm{per}(A)$, A a general complex matrix, is equal to the expectation of $(\det(B))^2$, where B is obtained from A by taking the square root of the minimal argument of each non-zero entry and then multiplying each non-zero entry by an element of $\{1,-1\}$ chosen independently uniformly at random. This leads to a Monte-Carlo algorithm for estimating the permanent (analysed first by Karmarkar, Karp, Lipton, Lovász and Luby).

Theorem 17. *Let A be a matrix and let B be the random matrix obtained from A by taking the square root of minimal argument of each non-zero entry and then multiplying each non-zero entry by an element of $\{1,-1\}$ chosen independently uniformly at random. Then $\mathbb{E}((\det(B))^2) = \mathrm{per}(A)$.*

Proof. Since $\det(B) = \sum_\pi \mathrm{sign}(\pi)\prod_i B_{i\pi(i)}$, we have

$$(\det(B))^2 = \sum_{(\pi_1,\pi_2)} \mathrm{sign}(\pi_1)\mathrm{sign}(\pi_2))\prod_i B_{i\pi_1(i)}B_{i\pi_2(i)} =$$

$$\sum_\pi \mathrm{sign}(\pi)^2 \prod_i B^2_{i\pi(i)} +$$

$$\sum_{(\pi_1,\pi_2);\pi_1\neq\pi_2} \mathrm{sign}(\pi_1)\mathrm{sign}(\pi_2))\prod_i B_{i\pi_1(i)}B_{i\pi_2(i)} =$$

$$\mathrm{per}(A) + \sum_{(\pi_1,\pi_2);\pi_1\neq\pi_2} \mathrm{sign}(\pi_1)\mathrm{sign}(\pi_2))\prod_i B_{i\pi_1(i)}B_{i\pi_2(i)}.$$

It remains to show that the expectation of the last sum is zero. Let A be an $n\times n$ matrix and let $\pi_1\neq\pi_2$ be two permutations of n. We can associate with them a graph $G(\pi_1,\pi_2)$. Its vertex-set is the set of all pairs (i,j) for $j=\pi_1(i)$ or $j=\pi_2(i)$. Two vertices $(i,j),(i',j')$ are connected by an edge if and only if $i=i'$ or $j=j'$. We recall that $c(G)$ denotes the number of the connected components of G.
Clearly, each $G(\pi_1,\pi_2)$ has at least one edge, and the non-empty components of each $G(\pi_1,\pi_2)$ are cycles of an even length. Let $\mathcal{G}$ be the set of all such graphs $G(\pi_1,\pi_2)$ for some $\pi_1\neq\pi_2$. If $G\in\mathcal{G}$ then we let $eq(G)=\{(\pi_1,\pi_2): G=G(\pi_1,\pi_2)\}$. We observe that $|eq(G)| = 2^{c(G)}$. Finally let us denote by $(ij)(G)$ an arbitrary vertex of G which belongs to a cycle. Now, we can write

$$\sum_{(\pi_1,\pi_2);\pi_1\neq\pi_2} \mathrm{sign}(\pi_1)\mathrm{sign}(\pi_2))\prod_i B_{i\pi_1(i)}B_{i\pi_2(i)} =$$

$$\sum_{G\in\mathcal{G}}\sum_{(\pi_1,\pi_2)\in eq(G)} \mathrm{sign}(\pi_1)\mathrm{sign}(\pi_2))\prod_i B_{i\pi_1(i)}B_{i\pi_2(i)} =$$

$$\sum_{G\in\mathcal{G}} B_{(ij)(G)}y(G),$$

where $y(G)$ is a random variable independent of $B_{(ij)(G)}$. Since the expectation of $B_{(ij)(G)}$ is equal to zero, the proof is finished. □

However, for the matrices with $0,1$ entries, there is something better. Jerrum, Sinclair and Vigoda constructed a *fully polynomial randomized approximation scheme* (FPRAS, in short) for approximating permanents of matrices with *nonnegative entries*. Briefly, a FPRAS for the permanent is an algorithm which, when given as input an $n \times n$ nonnegative matrix A together with an accuracy parameter $\epsilon \in (0,1]$, outputs a number Z (a random variable of the coins tossed by the algorithm) such that

$$\mathrm{Prob}[(1-\epsilon)Z \leq \mathrm{per}(A) \leq (1+\epsilon)Z] \geq \frac{3}{4}$$

and runs in time polynomial in $n, \sum |log(A_{ij})|$ and ϵ^{-1}. The probability $3/4$ can be increased to $1-\delta$ for any desired $\delta \in (0,1]$ by outputting the median of $O(\log \delta^{-1})$ independent trials.

10. Products over aperiodic closed walks

The following solution to the 2-dimensional Ising model has been developed by Kac, Ward and Feynman. This theory is closely related to that of Section 8. Let $G = (V,E)$ be a planar topological graph. It is convenient to associate a variable x_e instead of a weight to each edge e. If $e \in E$ then a_e will denote the orientation of e and a_e^{-1} will be the reversed orientation. We let $x_a = x_e$ for each orientation a of e. A circular sequence $p = v_1, a_1, v_2, a_2, ..., a_n, (v_{n+1} = v_1)$ is called a *prime reduced cycle*, if the following conditions are satisfied: $a_i \in \{a_e, a_e^{-1} : e \in E\}$, $a_i \neq a_{i+1}^{-1}$ and $(a_1, ..., a_n) \neq Z^m$ for some sequence Z and $m > 1$. We let $X(p) = \prod_{i=1}^n x_{a_i}$ and if each degree of G is at most 4 then we let $W(p) = (-1)^{\mathrm{rot}(p)} X(p)$ where $\mathrm{rot}(p)$ denotes the rotation. If $E' \subset E$ then we also let $X(E') = \prod_{e \in E'} x_e$. There is a natural equivalence on the prime reduced cycles: p is equivalent to reversed p. Each equivalence class has two elements and will be denoted by $[p]$. We let $W([p]) = W(p)$ and note that this definition is correct since equivalent walks have the same sign. The following theorem was proposed by Feynman and proved by Sherman. It provides, for a planar graph G, an expression for the generating function $\mathcal{E}(G,x)$ of the even sets of edges, in terms of the Ihara-Selberg function of G (see Definition 8.1).

Theorem 18. *Let G be a planar topological graph with each degree even and at most 4. Then*

$$\mathcal{E}(G,x) = \prod (1 - W([p])),$$

where we denote by $\prod(1 - W([p])$ the formal product of $(1 - W([p])$ over all equivalence classes of prime reduced cycles of G.

Note that the product is infinite even for a very simple graph consisting of one vertex and two loops.

When each transition between a pair of directed edges is decorated by its rotation contribution, Theorem 18 implies that $\mathcal{E}^2(G,x)$ becomes an Ihara-Selberg function (see Section 8). Hence we get the following corollary, whose statement (and incorrect proof) by Kac and Ward was in fact the starting point of the whole path approach.

Theorem 19. *Let G be a topological planar graph with all degrees even and at most 4. Then $\mathcal{E}^2(G,x)$ equals the determinant of the transition matrix between directed edges; each transition is decorated by its rotation contribution.*

Theorem 18 is formulated for those topological planar graphs where each degree is even and at most 4. It is not difficult to reduce $\mathcal{E}(G,x)$, G a general topological planar graph, to this case: First we make each degree even by doubling each edge. If we set the variables of the new edges to zero then each term containing a contribution of at least one new edge disappears. Next we make each non-zero degree equal to 2 or 4 as follows. We replace each vertex v with incident edges $e_1, ..., e_{2k}$, $k > 2$, listed in the circular order given by the embedding of G in the plane, by a path P of $2k-2$ vertices. We set the variables of the edges of P equal to 1. Next we double each edge of the unique perfect matching of P and set the variables of the new edges to zero. Finally we join the edges $e_1, ..., e_{2k}$ to the vertices of the auxiliary path so that the order is preserved along the path and each degree is four: there is a unique way to do that.
In order to prove Theorem 18, Sherman formulated and proved the following generalization which we now state. Let v be a vertex of degree 4 of G and let p be an aperiodic closed walk of G. We say that p satisfies the *crossover condition* at v if the way p passes through v is consistent with the crossover pairing of the four edges incident with v. Let U be a subset of vertices of degree 4. An even subset $E' \subset E$ is called *acceptable* for U if, for each $u \in U$ and for both pairs of edges incident with u and paired by the crossover pairing at u, if E' contains one edge of the pair then it also contains the other one.

Theorem 20. *Let $G = (V,E)$ be a topological planar graph where each degree is even and at most 4. Let U be a subset of vertices of G of degree 4. Let $\prod'_{G,U}(1 - W([p]))$ denote the product over all equivalence classes of the aperiodic closed walks of G which satisfy the crossover condition at each $u \in U$. Then*

$$\prod{}'_{G,U}(1 - W([p])) = \sum (-1)^{c(E')} X(E'),$$

where the sum is over all acceptable even subsets $E' \subset E$ and $c(E')$ is equal to the number of vertices of U such that E' contains all four edges incident with it.

The proof proceeds in two steps. First we show that, when the infinite product is expanded as a sum of monomials of variables, the coefficient corresponding to $X(E')$, for any E' acceptable for U, is equal to $(-1)^{c(E')}$. In the second step we show that all the remaining coefficients are zero.

Proposition 10.1. *Let E' be acceptable for U. If $\prod'_{G,U}(1 - W([p]))$ is expanded as a sum of monomials of variables then the coefficient of $X(E')$ is equal to $(-1)^{c(E')}$.*

Proof. By induction on the number of vertices of non-zero degree in E'. If E' has just one vertex then it consists of one loop e or two loops e, f and $c(E')$ equals zero or one. If E' consists of one loop only then $\prod'_{G,U}(1-W([p])) = (1+x_e)\times$ product of terms which cannot influence the coefficient at $X(E')$. If E' consists of two loops and $c(E') = 0$ then $\prod'_{G,U}(1 - W([p]))$ equals $(1 + x_e)(1 + x_f)(1 + x_e x_f)(1 - x_e x_f)\times$ product of terms which cannot influence the coefficient at $X(E')$. Finally let $c(E') = 1$ and E' consist of two loops. $\prod'_{G,U}(1 - W([p]))$ equals $(1 - x_e x_f)\times$ product of terms which cannot influence the coefficient at $X(E')$. Hence the base of the induction is verified.
Now we assume the statement is true for all acceptable subsets of edges with $n \geq 1$ vertices of non-zero degree. Let E' be an acceptable subgraph with $n + 1$ vertices of non-zero degree. A vertex v will be called *free* if it does not contribute to $c(E')$, i.e., if v has degree 2 in E' or $v \notin U$. Let $k = n + 1 - c(E')$ be the number of free vertices.
We continue by induction on k. First let $k = 0$, i.e., each vertex of non-zero degree in E' has degree 4 and belongs to U. The crossover conditions cause that there is a unique decomposition of E' into prime reduced cycles $p_1, ..., p_r$ such that $X(E') = \prod_{i=1}^{r} X(p_i)$. If $r = 1$ then $(-1)^{\mathrm{rot}(p_1)} = (-1)^{c(E')}$. If $r > 1$ then $\prod_{i=1}^{r}(-1)^{\mathrm{rot}(p_i)} = (-1)^{c(E')}$ since any two of the p_i's mutually intersect in an even number of vertices, and each vertex contributes to $c(E')$.
Hence let $k > 0$ and the statement holds for all acceptable subsets with less than k free vertices. If all free vertices have degree 2 in E' then we may proceed as in the case $k = 0$. Hence let v be a free vertex of E' of degree four in E'. We denote the edges incident with v by north, east, south and west according to the cyclic order induced by the embedding in the plane. We partition the prime reduced cycles of G which satisfy the crossover conditions at the vertices of U into four classes. Classes I,II,III contain prime reduced cycles that have an edge incident with v, and:

class I contains the prime reduced cycles that are consistent with west-north and east-south pairing,

class II contains the prime reduced cycles that are consistent with west-south and east-north pairing, class III contains the prime reduced cycles that are consistent with north-south and east-west pairing , and finally

class IV contains the prime reduced cycles that do not contain any edge incident with v.

Suppose $p \in I$ and $q \in II$. Then the product $W[p]W[q]$ contains a variable with the exponent bigger than 1. Hence it can make no contribution to $X(E')$. The same is true for II, III and I, II. Hence, if $\prod'_{G,U}(1-W([p])$ is expanded as a sum, the coefficient of $X(E')$ is the sum of the corresponding coefficients in $I \times IV$, $II \times IV$ and $III \times IV$. The contribution to $I \times IV$ can be regarded as the coefficient of $X(E'')$ in $\prod'_{G',U}(1 - W([p]))$ where G' and E'' are obtained from G and E' by deleting vertex v and by identifying the west, north edges into one edge, and the east, south edges into one edge. Analogously, we can treat the case $II \times IV$. Hence by the induction assumption the sum of the contributions from $I \times IV$ and $II \times IV$ is $2(-1)^{c(E')}$. The contribution to $III \times IV$ can be regarded as coming from $\prod'_{G,U\cup\{v\}}(1-W([p]))$, i.e. one additional cross-over condition is imposed, on vertex v. Using the induction assumption again (this time for k) we get that this contribution is equal to $(-1)^{c(E')+1}$.
Summarizing when the product $\prod'(1 - W([p]))$ is expanded as a sum, the coefficient of $X(E')$ is equal to $2(-1)^{c(E')} + (-1)^{c(E')+1}$, which we wanted to show.

□

To finish the proof of Theorem 20, we need to show that the remaining coefficients of the expansion of the infinite product are all equal to zero. We observe that the remaining coefficients belong to terms which are products of variables where at least one of the exponents is greater than 1.
We temporarily consider $\prod'_{G,U}(1 - W(p))$, where now the product is over prime reduced cycles and so it is the square of the original $\prod'_{G,U}(1 - W[p]))$. Let $a_1 > a_1^{-1} > ... > ...$ be a linear order of orientations of the edges of G.
Let A_1 be the set of all prime reduced cycles p such that a_1 appears in p. Each $p \in A_1$ has a unique factorization into words $(W_1, ..., W_k)$ each of which starts with a_1 and has no other appearance of a_1. Some of these words contain a_1^{-1} and some do not. We will need a lemma on coin arrangements stated below. The lemma was proved by Sherman. We present a proof based on the Witt identity from combinatorial group theory.
Witt Identity: Let $z_1, ..., z_k$ be commuting variables. Then

$$\prod_{m_1,...,m_k \geq 0} (1 - z_1^{m_1} \cdots z_k^{m_k})^{M(m_1,...,m_k)} = 1 - z_1 - z_2 - \ldots - z_k,$$

where $M(m_1, \dots, m_k)$ is the number of different non-periodic circular sequences made from the collection of m_i variables z_i, $i = 1, \cdots, k$.

Proof. (of Witt's identity) We take the inverse of both sides, expand and apply the Lyndon's Theorem 9.

□

Here comes the lemma. Suppose we have a fixed collection of N objects of which m_i are of ith kind, $i = 1, \dots, n$. Let b_k be the number of exhaustive unordered arrangements of these symbols into k disjoint, nonempty, circularly ordered sets such that no two circular orders are the same and none are periodic. For example suppose we have 10 coins of which 3 are pennies, 4 are nickles and 3 are quarters. The arrangement $\{(p, n), (n, p), (p, n, n, q, q, q)\}$ is not counted in b_3 since (p, n) and (n, p) represent the same circular order.

Lemma 10.2. *(On coin arrangements) If $N > 1$ then $\sum_{i=1}^{N} (-1)^i b_i = 0$.*

Proof. The lemma follows immediately if we expand the LHS of the Witt identity and collect the terms where the sums of the exponents of z_i's are the same.

□

Proposition 10.3. $\prod_{p \in A_1}(1 - W(p)) = 1 + x_{a_1} d_{11}$ *where d_{11} is a formal (possibly infinite) sum of monomials none of which has x_{a_1} as a factor.*

Proof. First we note that the additivity of rotation implies the following fact: if p_1, p_2 are two prime reduced cycles both containing a_1 and $p_1 p_2$ is also prime reduced then $(-1)^{\mathrm{rot}(p_1 p_2)} = (-1)^{\mathrm{rot}(p_1) + \mathrm{rot}(p_2)}$.
Let D be a monomial summand in the expansion of $\prod_{p \in A_1}(1 - W(p))$. Hence D is a product of finitely many $W(p), p \in A_1$. Each $p \in A_1$ has a unique factorization into words $(W_1, ..., W_k)$ each of which starts with a_1 and has no other appearance of a_1. Each word may appear several times in the factorization of p, and also in the factorization of different prime reduced cycles of A_1. Let $B(D)$ be the set-system of all the words (with repetition) appearing in the factorizations of the prime reduced cycles of D. It follows from the lemma on coin arrangements that the sum of all monomial summands D in the expansion of $\prod_{p \in A_1}(1 - W(p))$, which have the same $B(D)$ of more than one element, is zero. Hence the monomial summands D which survive in the expansion of $\prod_{p \in A_1}(1 - W(p)$ all have $B(D)$ consisting of exactly one word. This word may but need not contain a_1^{-1}. However, only the summands with their word NOT containng a_1^{-1} survive, by the following observation: If $b, c_1, ..., c_k$ are walks that contain neither a_1 nor a_1^{-1} then

$$W(a_1 b a_1^{-1} c_1 a_1^{-1} c_2 ... a_1^{-1} c_k) + W(a_1 b^{-1} a_1^{-1} c_1 a_1^{-1} c_2 ... a_1^{-1} c_k) +$$

$$W(a_1ba_1^{-1}c_1a_1^{-1}c_2...a_1^{-1}c_k^{-1}) + W(a_1b^{-1}a_1^{-1}c_1a_1^{-1}c_2...a_1^{-1}c_k^{-1}) = 0.$$

□

Analogously, let A_2 be the set of all prime reduced cycles p such that a_1^{-1} appears in p. Possibly $A_1 \cap A_2 \neq \emptyset$. Analogously as for $p \in A_1$, each $p \in A_2$ has a unique factorization into words $(W_1, ..., W_k)$ each of which starts with a_1^{-1} and has no other appearance of a_1^{-1}. Some of these words contain a_1 and some do not. The following proposition may be proved in exactly the same way as Proposition 10.3.

Proposition 10.4. *Let A_1, A_2 be as above. Then*

$$\prod_{p \in A_2}(1-W(p)) = \prod_{p \in A_1 \setminus A_2}(1-W(p)) = \prod_{p \in A_2 \setminus A_1}(1-W(p)) = \prod_{p \in A_1}(1-W(p)).$$

Let B be the set of prime reduced cycles in which neither a_1 nor a_1^{-1} appears. We may write

$$\prod_{p \in B}(1 - W(p)) = (1 + d_{12})^2,$$

where d_{12} is a formal sum of monomials, none of which has x_{a_1} as a factor. In $\prod_{p \in A_1}(1 - W(p)) \times \prod_{p \in A_2}(1 - W(p)) = (1 + x_{a_1}d_{11})^2$, the prime reduced cycles from $A_1 \cap A_2$ have been counted doubly, while the prime reduced cycles from $A_1 \setminus A_2$ and $A_2 \setminus A_1$ have been counted only once. Hence

$$\left(\prod_{p \in (A_1 \cup A_2)}(1 - W(p))\right)^2 =$$

$$\prod_{p \in A_1}(1-W(p)) \times \prod_{p \in A_2}(1-W(p)) \times \prod_{p \in A_1 - A_2}(1-W(p)) \times \prod_{p \in A_2 - A_1}(1-W(p)) =$$

$$(1 + x_{a_1}d_{11})^4.$$

Proof. (of Theorem 20)

$$\left(\prod\nolimits'_{G,U}(1 - W([p]))\right)^2 = \prod\nolimits'_{G,U}(1 - W(p)) =$$

$$\prod_{p \in (A_1 \cup A_2)}(1 - W(p)) \times \prod_{p \in B}(1 - W(p)) =$$

$$(1 + x_{a_1}d_{11})^2(1 + d_{12})^2,$$

and

$$\prod\nolimits'_{G,U}(1 - W([p])) = (1 + x_{a_1}d_{11})(1 + d_{12}).$$

Thus, there are no monomial summands having factors $x_{a_1}^n$, $n \geq 2$. The same argument disposes of the summands with factors $x_{a_i}^n$, $i \neq 1, n \geq 2$.

□

Theorem 20 can be used to express $\mathcal{E}(G,x)$ for general graphs as a linear combination of infinite products. A useful trick to obtain explicit formulas is to base such a linear combination on the genus. This we explain next. Let us first consider the graphs embeddable on torus (they are usually called *toroidal graphs*). We will again assume that each degree is even and at most 4. Let us take a natural representation of the torus as a rectangle with opposite edges identified. The edges of the original rectangle form two cycles on the torus. Let us call them the *vertical cycle*, and the *horizontal cycle*. Let G be a topological toroidal graph such that no vertex belongs to the horizontal or to the vertical cycle. If p is a prime reduced cycle of G, then let $h(p)$ denote the number of times p crosses the horizontal cycle, and let $v(p)$ denote the number of times p crosses the vertical cycle. The notation $h(E')$ and $v(E')$ is also used for even subsets E' of G. How do we define $\mathrm{rot}(p)$ on the torus? We unglue the edges of the rectangle which represents the torus. Hence each rectangle edge crossing now corresponds to 'leaving' the rectangle and 'coming back' to the rectangle by the opposite rectangle edge. If we draw all this in the plane, we get $h(G)v(G)$ crossings of the curves representing the edges of G. Let G' be the graph obtained from G by introducing a vertex to each such intersection. Note that G' is properly drawn in the plane and each degree of G' is even and at most four. Let us call the new vertices *special* and note that each special vertex has degree four in G'. Further note that each prime reduced cycle p of G corresponds to the prime reduced cycle p' of G' which satisfies the crossover condition at each special vertex. We let

$$(-1)^{\mathrm{rot}(p)} = (-1)^{h(p)+v(p)}(-1)^{\mathrm{rot}(p')}.$$

Finally we let

$$W_h(p) = (-1)^{h(p)}W(p),$$
$$W_v(p) = (-1)^{v(p)}W(p)$$

and

$$W_{h,v}(p) = (-1)^{h(p)+v(p)}W(p).$$

Hence

$$W([p']) = W_{h,v}([p]).$$

Theorem 21 and in particular Theorem 22 are based on the following curious lemma.

Lemma 10.5. *Let R be the set of all $0,1$-vectors of length $2n$ and let a be an arbitrary integer vector of length $2n$. Then*

$$2^{-n}(-1)^{\sum_{i=1}^{n} a_{2i-1}a_{2i}}\left(\sum_{r\in R}(-1)^{ra}(-1)^{s(r)}\right) = 1,$$

where $s(r)$ denotes the number of i such that $r_{2i-1} = r_{2i} = 1$.

Proof. We proceed by induction on n. The initial case $n = 1$ may be easily checked by hand. Next assume that Lemma 10.5 is true for n and we want to prove it for $n+1$. Let R' be the set of all $0,1$-vectors of length $2(n+1)$ and let a' be an arbitrary integer vector of length $2(n+1)$. Let a denote the initial part of a' of length $2n$. Then

$$2^{-n-1}(-1)^{\sum_{i=1}^{n+1} a'_{2i-1}a'_{2i}} \left(\sum_{r\in R'}(-1)^{ra'}(-1)^{s(r)}\right) =$$

$$2^{-1}(-1)^{a'_{2n+1}a'_{2n+2}}\alpha[(-1)^{a'_{2n+1}} + (-1)^{a'_{2n+2}} - (-1)^{a'_{2n+1}+a'_{2n+2}} + 1],$$

where

$$\alpha = 2^{-n}(-1)^{\sum_{i=1}^{n} a_{2i-1}a_{2i}} \left(\sum_{r\in R}(-1)^{ra}(-1)^{s(r)}\right).$$

By induction assumption we have that $\alpha = 1$ and applying again the first step of the induction, we find that the lemma holds.

□

Theorem 21. *If $G = (V, E)$ is a toroidal graph where each degree is even and at most four, then*

$$\mathcal{E}(G, x) =$$

$$1/2\left(\prod(1 - W_h([p])) + \prod(1 - W_v([p])) + \prod(1 - W_{h,v}([p])) - \prod(1 - W([p]))\right),$$

where $\prod$ is the product over all equivalence classes of prime reduced cycles of G.

Proof. Using Theorem 20 we get that

$$\prod(1 - W_{h,v}([p])) = \prod{}'(1 - W([p'])) = \sum(-1)^{h(E')v(E')}X(E'),$$

where the sum goes over all acceptable subgraphs E' of G', i.e. over all even subgraphs of G. Hence also

$$\prod(1 - W_v([p])) = \sum(-1)^{h(E')v(E')+h(E')}X(E'),$$
$$\prod(1 - W_h([p])) = \sum(-1)^{h(E')v(E')+v(E')}X(E'),$$

and

$$\prod(1 + W([p])) = \sum(-1)^{h(E')v(E')+h(E')+v(E')}X(E').$$

Let E' be an arbitrary even subset of G. Then the coefficient of $X(E')$ in

$$1/2\left(\prod(1 - W_h([p])) + \prod(1 - W_v([p])) + \prod(1 - W_{h,v}([p])) - \prod(1 - W([p]))\right)$$

equals

$$1/2(-1)^{h(E')v(E')}\left((-1)^{h(E')} + (-1)^{v(E')} - (-1)^{h(E')+v(E')} + 1\right) = 1,$$

by Lemma 10.5.

□

Using the machinery of *g-graphs* (see Definition 10.7), we can write down a formula for general graphs. The machinery is based on the following representation of orientable surfaces.

Definition 10.6. A highway surface S_g consists of a *base* B_0 and $2g$ *bridges* B^i_j, $i = 1, ..., g$ and $j = 1, 2$, where

(i) B_0 is a convex $4g$-gon with vertices $a_1, ..., a_{4g}$ numbered clockwise;
(ii) B^i_1, $i = 1, \cdots, g$, is a 4-gon with vertices $x^i_1, x^i_2, x^i_3, x^i_4$ numbered clockwise. It is glued with B_0 so that the edge $[x^i_1, x^i_2]$ of B^i_1 is identified with the edge $[a_{4(i-1)+1}, a_{4(i-1)+2}]$ of B_0 and the edge $[x^i_3, x^i_4]$ of B^i_1 is identified with the edge $[a_{4(i-1)+3}, a_{4(i-1)+4}]$ of B_0;
(iii) B^i_2, $i = 1, \cdots, g$, is a 4-gon with vertices $y^i_1, y^i_2, y^i_3, y^i_4$ numbered clockwise. It is glued with B_0 so that the edge $[y^i_1, y^i_2]$ of B^i_2 is identified with the edge $[a_{4(i-1)+2}, a_{4(i-1)+3}]$ of B_0 and the edge $[y^i_3, y^i_4]$ of B^i_2 is identified with the edge $[a_{4(i-1)+4}, a_{4(i-1)+5(mod 4g)}]$ of B_0.

We remark that in Definition 10.6 we denote by $[a, b]$ edges of polygons and not edges of graphs. The usual representation in the space of an orientable surface $\mathcal{S}$ of genus g may then be obtained from S_g by the following operation: for each bridge B, glue together the two segments which B shares with the boundary of B_0, and delete B.

Definition 10.7. A graph G is called a g-graph if it is embedded on S_g so that all the vertices belong to the base B_0, and each time an edge intersects a bridge, it crosses it completely.

This is analogous to the situation described earlier for the torus: we can imagine that we contract all the bridges (and get a usual representation of an orientable surface of genus g), draw our graph there, and then split the bridges back. The resulting drawing is a g-graph on S_g. If G is a g-graph and p is a prime reduced cycle of G then we denote by $a(p)$ the vector of length $2g$ such that $a(p)_{2(i-1)+j}$ equals the number of times p crosses bridge B^i_j, $i = 1, ..., g$, $j = 1, 2$. Similarly we will use the notation $a(E')$ where E' is an even subset of G.
Note that any graph G can be embedded as a g-graph where g is genus of G. As before, we only need to consider g-graphs that have all degrees even and at most four (by a remark after Theorem 18). We define $(-1)^{\mathrm{rot}(p)}$ analogously as for the torus: We consider G embedded in the plane by the projection of the bridges B^i_j outside B_0. We get $\sum_{i=1}^{g} a(G)_{2i-1}a(G)_{2i}$ crossings of the curves representing the edges of G. Let G' be the graph obtained from G by introducing a vertex to each such intersection. Note that G' is a topological planar graph, and each degree of G' is even and at most four. Let us call the new vertices

special and note that each special vertex has degree 4 in G'. Each non-periodic closed walk p of G corresponds to the prime reduced cycle p' of G' which satisfies the crossover condition at each special vertex. Let J denote the vector $(1,\dots,1)$ of all 1's. We define $(-1)^{\mathrm{rot}(p)}$ by

$$(-1)^{\mathrm{rot}(p')} = (-1)^{Ja(p)}(-1)^{\mathrm{rot}(p)}.$$

Let $R(g)$ denote the set of all $0,1$-vectors of length $2g$. For $r \in R(g)$ we let $W_r([p]) = (-1)^{ra(p)}W([p])$. Hence $W([p']) = W_J([p])$.

Theorem 22. *If $G = (V,E)$ is a g-graph where each degree is even and at most four, then*

$$\mathcal{E}(G,x) = 2^{-g}\sum_{r\in R(g)}(-1)^{s(J-r)}\prod(1-W_r([p])),$$

where $\prod$ is the formal infinite product over all equivalence classes of prime reduced cycles of G.

Proof. We proceed as in the proof of Theorem 21. Using Theorem 20 we get

$$\prod(1-W_J([p])) = \prod{}'(1-W([p'])) = \sum(-1)^{\sum_{i=1}^{g}a(E')_{2i-1}a(E')_{2i}}X(E'),$$

where the sum is over all acceptable subsets E'' of G', i.e., over all even subsets of G. Hence for $r \in R(g)$ we have

$$\prod(1-W_r([p])) = \sum(-1)^{\sum_{i=1}^{g}a(E')_{2i-1}a(E')_{2i}+(J-r)a(E')}X(E'),$$

where the sum is over all even subsets E' of G. Let E' be an arbitrary even subset of G. Then the coefficient of $X(E')$ in

$$2^{-g}\sum_{r\in R(g)}(-1)^{s(J-r)}\prod(1-W_r([p]))$$

is equal to

$$2^{-g}(-1)^{\sum_{i=1}^{g}a(E')_{2i-1}a(E')_{2i}}\sum_{r\in R(g)}(-1)^{(J-r)a(E')}(-1)^{s(J-r)} = 1,$$

by Lemma 10.5, since we can replace r by $J-r$ in the summation. $\square$

Dept. of Applied Mathematics and, Institute of Theoretical Computer Science (ITI), Charles University, Malostranske n. 25, 118 00 Praha 1, Czech Republic.

E-mail address: loebl@kam.mff.cuni.cz