Counting Points on Varieties over Finite Fields Related to a Conjecture of Kontsevich

John R. Stembridge

Department of Mathematics
University of Michigan
Ann Arbor, Michigan 48109–1109 USA
e-mail: jrs@math.lsa.umich.edu

Version of December 7, 1998

Contents

0. Introduction

Given a connected graph G, choose a variable for each edge, and consider the generating function for spanning trees of G, the weight of a spanning tree T being the product of the variables corresponding to edges *not* in T.

In 1997 at the Rutgers University Gelfand Seminar, M. Kontsevich proposed the conjecture that for every graph, the number of zeroes of this polynomial over the finite field $\mathbf{F}_q$ is a polynomial function of q. The motivation for the conjecture arose from the evaluation of certain integrals in quantum field theory.

R. Stanley has written a recent paper on various aspects of this conjecture [**St**]. He uses an inclusion-exclusion argument to show that Kontsevich's conjecture is true for all graphs if and only if the same is true when we modify the above generating function so that the weight of tree T is the product of the variables corresponding to edges that do

Partially supported by NSF Grant DMS–9700787 and RIMS, Kyoto University.
I would like to thank RIMS for their kind hospitality during the preparation of this article.

appear in T. Stanley has proved this modified conjecture for the complete graph (giving an explicit formula), and certain "nearly complete" graphs.

In this paper, we describe a simple technique that allows one to explicitly compute the number of points on certain very special varieties over finite fields $\mathbf{F}_q$, as a function of q. It is difficult to describe *a priori* the varieties for which this technique will succeed, but an obvious necessary condition is that the variety should be defined by the vanishing of integer polynomials that are linear with respect to most, if not all, of the dependent variables.

We have written a *Maple* program[1] that implements this method, and applied it to the varieties defined by spanning tree generating functions of graphs. To our surprise, it was very successful. For example, we used it to verify that Kontsevich's conjecture is true (or rather, Stanley's modification in which the spanning tree variables are used) for all graphs with at most 11 edges. By combining the program with some additional techniques, we are able to show that the conjecture is also true for graphs with 12 edges.

There is an interesting special case of the Kontsevich conjecture that can be formulated in terms of symmetric determinants [**St**, §3]. More specifically, consider a generic symmetric determinant in which certain off-diagonal entries have been specialized to 0. If the Kontsevich conjecture is true, then the number of points on the corresponding variety over $\mathbf{F}_q$ must be a polynomial function of q. Again, we applied our program to these varieties, and were able to verify the conjecture in the 6×6 case, as well as all cases with at most 11 off-diagonal variables.

On the other hand, if one drops the condition of symmetry in the above determinant, then the analogous conjecture fails, and we are able to show that the smallest counter-example is 7×7 and has 21 independent variables.

Another negative result occurs if one generalizes from graphs to matroids, as shown by Stanley. Even if we restrict to the class of regular (or unimodular) matroids, our program has found that the analogous conjecture fails.

1. A Probabilistic View

Rather than counting points on varieties over finite fields, there are some slight notational advantages that occur if we translate the problem into probabilistic language.

Given a set of polynomials $f_1, \ldots, f_k \in \mathbf{Z}[x_1, \ldots, x_m]$, we define $Z[f_1, \ldots, f_k](q)$ to be the probability that $f_i(x_1, \ldots, x_m) = 0$ for $1 \leqslant i \leqslant k$, where $x_1, \ldots, x_m$ are chosen uniformly at random from $\mathbf{F}_q$. In other words,

$$Z[f_1, \ldots, f_k](q) = q^{-m}|X_q|,$$

where X_q denotes the variety over $\mathbf{F}_q$ defined by the vanishing of $f_1, \ldots, f_k$.

[1]Available at `http://www.math.lsa.umich.edu/~jrs/`.

The main benefit of this notation is that it allows us to focus on the polynomials f_i and disregard the ambient space. The quantity $Z[x^2 - y^2](q)$ is the same whether we are interested in the variety $\{(x, y) \in \mathbf{F}_q^2 : x^2 = y^2\}$ or $\{(x, y, z) \in \mathbf{F}_q^3 : x^2 = y^2\}$.

For example, $Z[3](q) = 1$ if $3 \mid q$; otherwise $Z[3](q) = 0$.

PROPOSITION 1.1. *The quantity $Z[f_1, \ldots, f_k](q)$ is a polynomial function of q^{-1} if and only if $|X_q|$ is a polynomial function of q.*

Proof. Clearly $|X_q| \leqslant q^m$, so if $|X_q|$ is a polynomial, it must have degree $\leqslant m$. Hence the corresponding assertion about $Z[f_1, \ldots, f_k](q)$ follows immediately. Conversely, since $q^m Z[f_1, \ldots, f_k](q)$ is integer-valued for all prime powers q, it follows that if it is a Laurent polynomial in q, then it must also be a polynomial in q. $\square$

A (non-empty) polynomial list $[f_1, \ldots, f_k]$ is said to be *primitive* if there is no prime integer that divides all of the coefficients.

PROPOSITION 1.2. *If $[f_1, \ldots, f_k]$ is primitive, then $Z[f_1, \ldots, f_k](q) = O(q^{-1})$.*

Proof. Proceed by induction with respect to the number of variables that appear among $f_1, \ldots, f_k$, say m. If $m = 0$, then the f_i's are a collection of scalars with no common divisor, and hence $Z[f_1, \ldots, f_k] = 0$. Otherwise, $m > 0$ and we may choose a variable x that appears in one or more of the f_i's. Let $g_1, \ldots, g_l$ denote the coefficients of the f_i's as polynomials in x. Since $[f_1, \ldots, f_k]$ is primitive, the same is true of $[g_1, \ldots, g_l]$.

If we choose a random point in $\mathbf{F}_q^{m-1}$ and evaluate $f_1, \ldots, f_k$, we obtain a collection of univariate polynomials in x. These polynomials will be identically 0 with probability $Z[g_1, \ldots, g_l]$. Otherwise, to obtain 0's, x must be a root of one or more polynomials of degree $\leqslant d$, where d denotes the maximum degree of the (unevaluated) f_i's with respect to x, an event with probability at most d/q. Hence

$$Z[f_1, \ldots, f_k](q) \leqslant dq^{-1} + Z[g_1, \ldots, g_l](q)$$

and the result follows by induction. $\square$

Now consider the consequences if f_1 is linear with respect to some variable x_1; i.e.,

$$f_1 = g_0 + g_1 x_1, \quad g_i \in \mathbf{Z}[x_2, x_3, \ldots]. \tag{1.1}$$

Given a polynomial $h = h_0 + h_1 x_1 + \cdots + h_k x_1^k$ with $h_i \in \mathbf{Z}[x_2, x_3, \ldots]$, $h_k \neq 0$, define

$$\bar{h} = h_0 g_1^k - h_1 g_0 g_1^{k-1} + \cdots + (-1)^k h_k g_0^k \ \in \mathbf{Z}[x_2, x_3, \ldots]. \tag{1.2}$$

This can be viewed as a fraction-free resultant of h and f_1.

Proposition 1.3. *Assuming f_1 satisfies (1.1), then*

$$Z[f_1,\dots,f_k] = Z[g_0,g_1,f_2,\dots,f_k] + q^{-1}Z[\bar f_2,\dots,\bar f_k] - q^{-1}Z[g_1,\bar f_2,\dots,\bar f_k],$$

where $\bar f_2,\dots,\bar f_k$ are defined as in (1.2).

Proof. Partition the points in X_q according to whether $g_1 = 0$ or $g_1 \neq 0$. In the former case, we have $f_1 = 0$ if and only if $g_0 = 0$, and the probability that a randomly chosen point in $\mathbf{F}_q^m$ lies in this subvariety is $Z[g_0,g_1,f_2,\dots,f_k](q)$.

Otherwise, if $g_1 \neq 0$, we must have $x_1 = -g_0/g_1$ in order to satisfy $f_1 = 0$. Since $\bar f_i$ is g_1^k times the result of substituting $x_1 = -g_0/g_1$ in f_i, it follows (given $f_1 = 0$ and $g_1 \neq 0$) that $f_i = 0$ if and only if $\bar f_i = 0$. Ignoring the variable x_1, the probability that a randomly chosen point in $\mathbf{F}_q^{m-1}$ satisfies $g_1 \neq 0$ and $\bar f_2 = \cdots = \bar f_k = 0$ is

$$Z[\bar f_2,\dots,\bar f_k] - Z[g_1,\bar f_2,\dots,\bar f_k].$$

If we restore x_1 and add the condition $f_1 = 0$, then the probability drops by a factor of q since x_1 is uniquely determined. □

Remark 1.4. We can simplify the last term in the above recurrence, based on the observation that $\bar h = \pm h_k g_0^k \bmod g_1$. Indeed,

$$Z\big[g_1,\bar f_2,\dots,\bar f_k\big] = Z\big[g_1,\hat f_2 g_0^{\varepsilon(f_2)},\dots,\hat f_k g_0^{\varepsilon(f_k)}\big],$$

where $\hat h$ denotes the leading term of h as a polynomial in x_1, and $\varepsilon(h) = 0$ or 1 according to whether h is independent of x_1.

2. The Conjecture of Kontsevich

In the present context, graphs are unoriented and may have loops and multiple edges. It will be helpful to regard the edge set of a graph as the "ground set," with the vertices providing incidence data.

Given a graph G, choose a variable x_e for each edge e and define

$$\Sigma(G) = \sum_T \prod_{e\in T} x_e,$$

where T ranges over all spanning trees of G. If G is disconnected, $\Sigma(G) = 0$.

For any edge e, we let $G-e$ denote the graph obtained by deleting e, and G/e the graph obtained by contracting e to a point. By partitioning the spanning trees of G according to whether they contain e, one can see that

$$\Sigma(G) = \begin{cases} \Sigma(G/e)\cdot x_e + \Sigma(G-e) & \text{if } e \text{ is not a loop,} \\ \Sigma(G-e) & \text{otherwise.} \end{cases} \tag{2.1}$$

With suitable initial conditions, this could serve as the definition of $\Sigma(G)$.

Translating the (modified) conjecture of Kontsevich reported in [**St**], we arrive at

CONJECTURE 2.1. *For all graphs G, $Z[\Sigma(G)](q)$ is a polynomial function of q^{-1}.*

We claim that $Z[\Sigma(G)]$ is unchanged by the addition or deletion of loops or duplicate edges. In the case of a loop, this is clear since $\Sigma(G)$ does not depend on any loop variables. If e and e' are edges of G with the same endpoints, then $\Sigma(G)$ is a function of $x_e + x_{e'}$ and the remaining variables. Furthermore, as x_e and $x_{e'}$ vary uniformly over $\mathbf{F}_q^2$, one sees that $x_e + x_{e'}$ varies uniformly over $\mathbf{F}_q$, so the claim follows. Hence there is no loss of generality in restricting our attention to simple graphs (i.e., no loops or multiple edges).

Unless stated otherwise, assume henceforth that G is a simple, connected graph.

Another easy observation to make is that if G has a cut vertex (i.e., a vertex whose removal disconnects G), then the edges of G can be partitioned into two subgraphs G_1 and G_2 with the property that $\Sigma(G) = \Sigma(G_1) \cdot \Sigma(G_2)$, whence

$$Z[\Sigma(G)] = Z[\Sigma(G_1)] + Z[\Sigma(G_2)] - Z[\Sigma(G_1)] \cdot Z[\Sigma(G_2)]. \tag{2.2}$$

Thus to prove Conjecture 2.1, it suffices to consider 2-connected graphs.

LEMMA 2.2. *For any edge e of G, we have*

$$Z[\Sigma(G)] = q^{-1} - q^{-1} Z[\Sigma(G/e)] + Z[\Sigma(G/e), \Sigma(G-e)]. \tag{2.3}$$

Proof. Proposition 1.3 and (2.1). $\square$

LEMMA 2.3. *For any $a, b, c, d \in \mathbf{Z}[x_1, x_2, \ldots]$, we have*

$$Z[ay+b, cy+d] = Z[a,b,c,d] + q^{-1} Z[ad-bc] - q^{-1} Z[a,c].$$

Proof. Applying Proposition 1.3 twice, we obtain

$$\begin{aligned} Z[ay+b, cy+d] &= Z[a,b,cy+d] + q^{-1} Z[ad-bc] - q^{-1} Z[a, ad-bc] \\ &= Z[a,b,c,d] + q^{-1} Z[a,b] - q^{-1} Z[a,b,c] + q^{-1} Z[ad-bc] - q^{-1} Z[a,bc] \\ &= Z[a,b,c,d] + q^{-1} Z[ad-bc] - q^{-1} Z[a,c], \end{aligned}$$

the last equality being a consequence of $Z[a,bc] = Z[a,b] + Z[a,c] - Z[a,b,c]$. $\square$

THEOREM 2.4. *For any (distinct) edges e, e' of G, we have*

$$Z[\Sigma(G)] = q^{-1} + q^{-2} - q^{-1}Z[\Sigma(G/e)] - q^{-1}Z[\Sigma(G/e')] - q^{-2}Z[\Sigma(G/e/e')] \\ + q^{-1}Z[\Delta_{e,e'}(G)] + Z[\Sigma(G/e/e'), \Sigma(G/e-e'), \Sigma(G/e'-e), \Sigma(G-e-e')],$$

where $\Delta_{e,e'}(G) = \Sigma(G/e-e') \cdot \Sigma(G/e'-e) - \Sigma(G/e/e') \cdot \Sigma(G-e-e')$.

Proof. Using Lemma 2.3 (with $y = x_{e'}$) to compute $Z[\Sigma(G/e), \Sigma(G-e)]$, we find

$$Z[\Sigma(G/e), \Sigma(G-e)] = Z[\Sigma(G/e/e'), \Sigma(G/e-e'), \Sigma(G/e'-e), \Sigma(G-e-e')] \\ + q^{-1}Z[\Delta_{e,e'}(G)] - q^{-1}Z[\Sigma(G/e'/e), \Sigma(G/e'-e)],$$

using the fact that deletion and contraction commute (e.g., $(G-e)/e' = G/e'-e$). Applying Lemma 2.2 to G/e', we can eliminate the appearance of $Z[\Sigma(G/e'/e), \Sigma(G/e'-e)]$ from the above expression, obtaining

$$Z[\Sigma(G/e), \Sigma(G-e)] = Z[\Sigma(G/e/e'), \Sigma(G/e-e'), \Sigma(G/e'-e), \Sigma(G-e-e')] \\ + q^{-1}Z[\Delta_{e,e'}(G)] + q^{-2} - q^{-1}Z[\Sigma(G/e')] - q^{-2}Z[\Sigma(G/e/e')].$$

Now substitute the result back into (2.3). $\square$

We remark that in the above proof, applying Lemma 2.2 to G/e' is somewhat sloppy, since G/e' need not be a simple graph. However, the validity of Lemma 2.2 depends only on e not being a loop.

A particularly interesting situation occurs when $\{e, e'\}$ is a cutset; i.e., $G-e-e'$ is disconnected. For simplicity, we may assume that this is a minimal cutset; otherwise G has a cut vertex and (2.2) applies. In that case, $G/e-e'$ and $G/e'-e$ have the same 2-connected components, and hence $\Sigma(G/e-e') = \Sigma(G/e'-e)$. It follows that $Z[\Sigma(G/e)] = Z[\Sigma(G/e')]$ (Lemma 2.2), and since $\Sigma(G-e-e') = 0$,

$$\Delta_{e,e'}(G) = \Sigma(G/e-e') \cdot \Sigma(G/e'-e) = \Sigma(G/e-e')^2. \tag{2.4}$$

Furthermore, the last term in Theorem 2.4 reduces to $Z[\Sigma(G/e/e'), \Sigma(G/e-e')]$, and hence can be eliminated via Lemma 2.2. Combining these simplifications, Theorem 2.4 implies

$$Z[\Sigma(G)] = q^{-2} + (1-2q^{-1})Z[\Sigma(G/e)] \\ + (q^{-1} - q^{-2})Z[\Sigma(G/e/e')] + q^{-1}Z[\Sigma(G/e-e')]. \tag{2.5}$$

COROLLARY 2.5. *A minimal graph that provides a counterexample to Conjecture 2.1 must have edge connectivity* $\geqslant 3$.

It is well-known that the spanning tree generating function of a graph is expressible as a determinant. Define the Laplacian $L(G)$ to be a matrix whose rows and columns are indexed by the vertices of G, with the (u,v)-entry being $-x_{uv}$ (if $u \neq v$ and $uv = vu$ is an edge of G), or 0 (if u and v are non-adjacent), or $\sum x_{uv'}$, summed over all vertices v' adjacent to u (if $u = v$). The Matrix-Tree Theorem (e.g., [**L**, §4]) asserts that

$$\Sigma(G) = \det L_{v,v}(G) \tag{2.6}$$

for any vertex v, where $L_{u,v}(G)$ denotes the result of deleting from $L(G)$ the row indexed by u and the column indexed by v.

Following Stanley (see Theorem 3.3 of [**St**]), we observe that for each vertex u adjacent to v, the variable x_{uv} appears only once in $L_{v,v}(G)$, in the (u,u)-entry. Thus as x_{uv} varies uniformly over $\mathbf{F}_q$, the (u,u)-entry also varies uniformly over $\mathbf{F}_q$. It follows that if $\bar{L}_{v,v}(G)$ is the matrix obtained from $L_{v,v}(G)$ by redefining the (u,u)-entry to be x_u for all u adjacent to v, then $\det \bar{L}_{v,v}(G)$ and $\det L_{v,v}(G)$ vanish with the same probability; i.e.,

$$Z[\Sigma(G)] = Z[\det \bar{L}_{v,v}(G)]. \tag{2.7}$$

For any vertex u, we let $N(u)$ denote the neighborhood of u; i.e., the set consisting of u and all vertices adjacent to u.

THEOREM 2.6. *If u, u', v, v' are vertices that form a complete subgraph of G and $N(u)$ is a subset of both $N(v)$ and $N(v')$, then*

$$Z[\Sigma(G)] = Z[\Sigma(G - u'v')] + q^{-1}Z[\Sigma(G - u'u)] - q^{-1}Z[\Sigma(G - u'u - u'v')].$$

Proof. If we set $x_{u'u} = 0$ in $\bar{L}_{v,v}(G)$, we obtain $\bar{L}_{v,v}(G - u'u)$, so by (2.7)

$$Z[\Sigma(G)](q) - q^{-1}Z[\Sigma(G - u'u)](q)$$

represents the simultaneous probability that $\det \bar{L}_{v,v}(G) = 0$ and that the (u',u)-entry of $\bar{L}_{v,v}(G)$ is invertible in $\mathbf{F}_q$. In that event, there is a uniquely determined multiple of the row and column indexed by u that can be added to the row and column indexed by v' so that the (u',v')-entry is zero.

Consider the effect of this operation on the distribution of the entries of the matrix. Of course the matrix remains symmetric, the determinant is preserved, and only the row and column indexed by v' is modified. First consider a typical off-diagonal entry in the

v' column; say (w, v'). In order for this entry to be modified, we must have $w \in N(u)$, so in particular (since $N(u) \subseteq N(v')$), w must be adjacent to v', and the (w, v')-entry is originally $-x_{wv'}$. Since w and v' are both in $N(u)$, and hence $N(v)$, it follows that the variable $x_{wv'}$ does not appear anywhere else in $\bar{L}_{v,v}(G)$, aside from the identical (v', w)-entry. Thus any quantities added to this entry (except in the case $w = u'$) do not change the fact that it is distributed uniformly over $\mathbf{F}_q$ and independent of the other entries. There is a similar argument for the (v', v')-entry, since it is originally a variable that is independent of all other entries.

Thus when the (u', u)-entry is restricted to be invertible in $\mathbf{F}_q$, the distributions of $\det \bar{L}_{v,v}(G)$ and $\det \bar{L}_{v,v}(G - u'v')$ are the same, which implies

$$Z[\Sigma(G)] - q^{-1}Z[\Sigma(G - u'u)] = Z[\Sigma(G - u'v')] - q^{-1}Z[\Sigma(G - u'u - u'v')],$$

given the observation made at the beginning of the argument. □

COROLLARY 2.7. *A minimal graph that provides a counterexample to Conjecture 2.1 cannot have a triple of vertices u, v, v' such that $N(u) \subseteq N(v), N(v')$.*

Proof. Given the stated condition, u, v, and v' must be mutually adjacent. If u is adjacent to no other vertices, then the edges uv and uv' form a (minimal) cutset, whence (2.5) is applicable. Otherwise, there is another vertex u' adjacent to u, and hence also adjacent to v and v', so Theorem 2.6 is applicable. □

Extending our previous notation, define (for example) $L_{uv,u'v'}(G)$ to be the matrix obtained from $L(G)$ by deleting the rows indexed by u and v, and the columns indexed by u' and v'. Recall that a key step in the derivation of Corollary 2.5 is the fact that if $\{e, e'\}$ is a minimal cutset for G, then $\Delta_{e,e'}(G)$ is a perfect square (see (2.4)). The following result shows that this is true in general.

THEOREM 2.8. *Let e, e' be distinct edges of G.*

(a) *If $e = uv$ and $e' = u'v$, then*

$$\Delta_{e,e'}(G) = \det L_{uv,u'v}(G)^2.$$

(b) *If $e = uv$ and $e' = u'v'$ (and u, v, u', v' are distinct), then*

$$\Delta_{e,e'}(G) = \big(\det L_{uv,u'v}(G) - (-1)^r \det L_{uv,v'v}(G)\big)^2,$$

where r denotes the distance between rows u' and v' in $L_{v,v}(G)$.

Proof. (a) Recall that $\Sigma(G/e)$ and $\Sigma(G-e)$ are the linear and constant terms of $\Sigma(G)$ with respect to x_e. Since the variables x_e and $x_{e'}$ appear only in the rows and columns of $L_{v,v}(G)$ indexed by u and u' (respectively), it follows from (2.6) that

$$\Sigma(G/e-e') = \det L_{uv,uv}(\hat{G}), \qquad \Sigma(G/e'-e) = \det L_{u'v,u'v}(\hat{G}),$$
$$\Sigma(G/e/e') = \det L_{uu'v,uu'v}(\hat{G}), \quad \Sigma(G-e-e') = \det L_{v,v}(\hat{G}),$$

where $\hat{G} = G-e-e'$. However, by the Dodgson determinant identity [**D**], one knows that for all $i<k$ and $j<l$ (or vice-versa),

$$A_{i,l}A_{k,j} = A_{i,j}A_{k,l} - A_{ik,jl}A_{\emptyset,\emptyset},$$

where $A_{I,J}$ denotes the minor of a square matrix A obtained by deleting the rows indexed by I and the columns indexed by J. Hence

$$\Delta_{e,e'}(G) = \det L_{uv,u'v}(\hat{G}) \det L_{u'v,uv}(\hat{G}) = \det L_{uv,u'v}(G)^2,$$

since $L(G)$ is symmetric and $L_{uv,u'v}(G)$ is independent of x_e and $x_{e'}$.

(b) We may assume that u' and v' index consecutive rows and columns of $L_{v,v}(G)$, for if we interchange the row and column of u' with an adjacent row and column other than v', the parity of r changes, and the determinant of $L_{uv,v'v}(G)$ changes sign. The analysis is now similar to (a), the only difference being that the variable $x_{e'}$ appears in four positions (the rows and columns of u' and v'), which leads to

$$\Sigma(G/e'-e) = \det L_{u'v,u'v}(\hat{G}) + \det L_{u'v,v'v}(\hat{G}) + \det L_{v'v,u'v}(\hat{G}) + \det L_{v'v,v'v}(\hat{G}).$$

Similarly $\Sigma(G/e/e')$ can be obtained by deleting the row and column of u from these four minors. Thus via four applications of the Dodgson identity, we obtain

$$\begin{aligned}\Delta_{e,e'}(G) &= \big(\det L_{uv,u'v}(\hat{G}) + \det L_{uv,v'v}(\hat{G})\big) \cdot \big(\det L_{u'v,uv}(\hat{G}) + \det L_{v'v,uv}(\hat{G})\big) \\ &= \big(\det L_{uv,u'v}(G) + \det L_{uv,v'v}(G)\big)^2,\end{aligned}$$

again by the symmetry of $L(G)$. Although the determinants of $L_{uv,u'v}(G)$ and $L_{uv,v'v}(G)$ both depend on $x_{e'}$, it is easily shown that their sum does not. $\square$

We remark that Tim Chow [**C**] has given a combinatorial interpretation of $\Delta_{e,e'}(G)$ based on the above formula. It seems plausible that a combinatorial derivation could be obtained along the lines of Zeilberger's proof of the Dodgson identity [**Z**].

3. Duality

Let $\bar{\Sigma}(G)$ denote the generating function for complements of spanning trees; i.e.,

$$\bar{\Sigma}(G) := \sum_T \prod_{e \in G - T} x_e,$$

where T ranges over all spanning trees of G. The conjecture that $Z[\bar{\Sigma}(G)](q)$ should be a polynomial function of q^{-1} for all graphs G is essentially the original formulation of Kontsevich's conjecture (cf. also §7B).

Given a subset S of the edge set of G, extend the notation of §2 by defining G/S to be the graph obtained from G by contracting the edges of S to points. A *minor* of G is obtained by any sequence of deletions or contractions of edges of G.

The following is a more explicit version of Proposition 2.1 in [**St**].

Proposition 3.1. *We have*

$$1 - Z[\bar{\Sigma}(G)] = \sum_T \sum_S (-1)^{|S|} q^{-|S|-|T|} \big(1 - Z[\Sigma(G/T - S)]\big),$$

where the outer sum ranges over edge subsets T of G without cycles, and the inner sum ranges over edge subsets S of G/T.

Proof. For edge subsets T of G, define $N_{G,T}(q)$ to be the probability in $\mathbf{F}_q$ of the event that (1) $\Sigma(G) \neq 0$ and (2) $x_e = 0$ if and only if $e \in T$. Similarly define $\bar{N}_{G,T}(q)$, substituting $\bar{\Sigma}(G)$ in place of $\Sigma(G)$. Since

$$\bar{\Sigma}(G) \cdot \prod_{e \in G} x_e^{-1} = \Sigma(G)|_{x_e \to 1/x_e},$$

it follows that $N_{G,\emptyset}(q) = \bar{N}_{G,\emptyset}(q)$.

If we substitute $x_e = 0$ in $\bar{\Sigma}(G)$ for all $e \in T$, we obtain 0 if there is a cycle in T; otherwise, we obtain $\bar{\Sigma}(G/T)$. Hence

$$1 - Z[\bar{\Sigma}(G)] = \sum_T \bar{N}_{G,T}(q) = \sum_{T \text{ acyclic}} q^{-|T|} \bar{N}_{G/T,\emptyset}(q) = \sum_{T \text{ acyclic}} q^{-|T|} N_{G/T,\emptyset}(q).$$

However by inclusion-exclusion, we have

$$N_{G/T,\emptyset}(q) = \sum_S (-q)^{-|S|} \big(1 - Z[\Sigma(G/T - S)]\big),$$

so the claimed identity follows. $\square$

There is a similar inversion formula expressing $Z[\Sigma(G)]$ as an alternating sum of terms of the form $Z[\bar{\Sigma}(H)]$, where H ranges over minors of G.

COROLLARY 3.2. *If $Z[\Sigma(H)](q)$ is a polynomial in q^{-1} for every minor H of G, then the same is true for $Z[\bar{\Sigma}(H)](q)$.*

If G has n vertices and at most $2n-3$ edges, then a spanning tree has more edges than its complement in G. In these cases, it may be easier to test whether $Z[\bar{\Sigma}(G)]$ is a polynomial, rather than $Z[\Sigma(G)]$.

COROLLARY 3.3. *If G is a minimal counterexample to Conjecture 2.1, then $Z[\bar{\Sigma}(G)](q)$ is not a polynomial in q^{-1}, and is minor-minimal with respect to this property.*

4. A Reduction Method

We now turn to the problem of explicitly computing $Z[\Sigma(G)](q)$, or more generally $Z[f_1, \ldots, f_k](q)$, regarding q as an indeterminate. Motivated by the reasoning used in the proof of Theorem 2.4, we define a *reduction* of the expression $Z[f_1, \ldots, f_k]$ to be an application of one or more of the following relations:

(R1) If one of the polynomials, say f_1, is linear with respect to one of the variables, say x_1, then we can apply the relation of Proposition 1.3.

(R2) If one of the polynomials, say f_1, factors nontrivially over **Z**; i.e., $f_1 = g_1 g_2$, where $g_i \in \mathbf{Z}[x_1, x_2, \ldots]$ and $g_i \neq 0, \pm 1$, then we have the relation

$$Z[f_1, \ldots, f_k] = Z[g_1, f_2, \ldots, f_k] + Z[g_2, f_2, \ldots, f_k] - Z[g_1, g_2, f_2, \ldots, f_k].$$

(R3) If two of the polynomials, say f_1, f_2, are scalars (i.e., integers), then we have

$$Z[f_1, \ldots, f_k] = Z[\gcd(f_1, f_2), f_3, \ldots, f_k].$$

(R4) If $f_1 = \pm f_2$ or $f_1 = 0$ (say), then $Z[f_1, \ldots, f_k] = Z[f_2, \ldots, f_k]$.

(R5) If $f_i = \pm 1$ for some i, then $Z[f_1, \ldots, f_k] = 0$.

More generally, we define reductions of $\mathbf{Z}[q^{-1}]$-linear combinations of expressions of the form $Z[f_1, \ldots, f_k]$ in the obvious way.

If none of the above relations can be applied, then we say that $[f_1, \ldots, f_k]$ is *inert.*[2] To abuse notation, we may also say that $Z[f_1, \ldots, f_k]$ is inert. More generally, any $\mathbf{Z}[q^{-1}]$-linear combination of inert expressions is said to be inert.

It is easy to see that $[f_1, \ldots, f_k]$ is inert if and only if at most one of the f_i's is a prime integer and the remaining f_i's are distinct (up to a factor of ± 1), irreducible, primitive polynomials of degree at least two with respect to every dependent variable.

[2]It is unfortunate that the term "irreducible" already has a standard meaning for varieties.

Of special importance is the empty list $[\ ]$, for which we have $Z[\ ](q) = 1$. We say that $[f_1, \ldots, f_k]$ is *completely reducible* if $Z[f_1, \ldots, f_k]$ can be reduced to a $\mathbf{Z}[q^{-1}]$-multiple of $Z[\ ]$. Of course in this case, Proposition 1.1 implies that the number of points on the corresponding variety over $\mathbf{F}_q$ is a polynomial function of q.

Although we have defined the above relations as "reductions," it requires some work to show that there are no infinite sequences of reductions. To verify this claim, let us first define an *offspring* of the nonzero polynomial f to be either a non-trivial divisor of f (i.e., not ± 1 or $\pm f$), or the linear or constant term with respect to some variable that appears in f. The zero polynomial has no offspring, by definition.

LEMMA 4.1. *There are no infinite sequences $g_1, g_2, \ldots$ in which g_{k+1} is an offspring of g_k, for all k.*

Proof. If we order $\mathbf{Z}[x_1, x_2, \ldots]$ first by total degree, and second by the number of dependent variables, then an offspring of f might not (strictly) precede f in this ordering only if f is a constant. However in that case, the only offspring of f are strictly smaller than f in absolute value. $\square$

PROPOSITION 4.2. *Starting from any polynomial list $F = [f_1, \ldots, f_k]$, the reductions (R1)–(R5) can only be applied a finite number of times.*

Proof. Set $F_1 = F$, and given F_i, let F_{i+1} be the polynomial list corresponding to one of the terms appearing on the right hand side of one of the relations (R1)–(R4). (An application of (R5) is clearly terminal.) If the proposition were false, there would exist an infinite sequence $F_1, F_2, \ldots$ of this type. Indeed, any infinite rooted tree of bounded width has an infinite chain.

Observe that every term on the right hand sides of (R1)–(R4) involves the same or a smaller set of variables, and the two terms of (R1) involving $[\bar{f}_2, \ldots, \bar{f}_k]$ and $[g_1, \bar{f}_2, \ldots, \bar{f}_k]$ (see Proposition 1.3) both have a strictly smaller set of variables. Hence these terms can be chosen only a finite number of times in any sequence $\{F_i\}_{i \geqslant 1}$. By truncating an initial segment if necessary, we may assume that $\{F_i\}_{i \geqslant 1}$ is constructed without ever selecting these particular right hand sides.

If F_{i+1} is obtained from F_i via (R1), the remaining possibility is that two of the members of F_{i+1} are offspring of one of the members of F_i, and the remaining terms are identical. Similarly, if (R2) is applied, one member of F_i is replaced with one or two of its offspring. The remaining relations all involve deletion of terms or replacements of scalars, so for each non-constant polynomial f appearing in F_i we can trace a sequence from f back to some f_j in F in which each term is either equal to, or an offspring of, the previous term. But every offspring-sequence starting at f_j must be finite (Lemma 4.1), so there can only be finitely many occasions in the sequence $\{F_i\}_{i\geqslant 1}$ in which offspring of non-constant polynomials are chosen.

Thus by truncation, we may assume that all applications of (R1)–(R4) involve deleting terms or replacing scalars with divisors. However it is easy to see that no infinite sequence of reductions can be constructed from these limited operations. $\square$

5. Conducting a Search

We have implemented an algorithm in *Maple* for reducing any expression $Z[f_1,\dots,f_k]$ to a $\mathbf{Z}[q^{-1}]$-linear combination of inert expressions. In theory this is straightforward, since one needs only to look for opportunities to apply (R1)–(R5), and halt when no such opportunities exist. However in practice, there are a number of subtle points, one being the need to guard against expression swell, and another being the fact that while a given expression may be completely reducible, it may also be difficult to find a sequence of reductions that achieve this. The latter is the primary objective of the computation.

A. Strategy.

We summarize here the main features of our strategy for finding complete reductions.

1. One should keep the terms f_i in a canonical order, and replace f_i with $-f_i$ in case the leading coefficient of f_i is negative. Using (R3), one may permit at most one scalar among the f_i's. With these conventions, we increase the likelihood of finding cancellations such as $Z[f]-Z[-f]=0$.

2. Whenever using (R1) to eliminate a variable, the new polynomials that are introduced are replaced with their "square-free" parts. More specifically, if the polynomial g is to be introduced into an expression $Z[g,\dots]$, we first compute the canonical square-free factorization $g=cg_1g_2^2g_3^3\cdots$, where the g_i's are primitive, co-prime, and square-free, and c is an integer. (This is significantly cheaper than an irreducible factorization of g.) We then replace g with $cg_1g_2g_3\cdots$, an operation that is easily shown to be a reduction in the sense of §4.

3. The main issue of strategy concerns how to choose from among the many opportunities that may exist for applying (R1) and (R2). Since the use of (R1) tends to produce expressions with fewer variables than the original, this operation is usually preferable to (R2). However, it can easily lead to expressions large enough to exceed the capacity of *Maple*. It is also difficult to determine in advance which variable and which term f_i will yield the smallest results. On the other hand, if we apply (R2) whenever possible, the total number of terms tends to explode.

To cope with these conflicting tendencies, we use a heuristic that combines randomized, greedy, and conservative methods. The algorithm first looks for a greedy solution by

	8	9	10	11	12	13
5	1					
6		2	4	3	1	
7				4	15	22
8					4	32

TABLE I. Potential counterexamples to Conjecture 2.1.

attempting a complete reduction of $Z[f_1, \ldots, f_k]$, using (R1) first whenever possible. When there is a choice of variables to eliminate, one is taken at random. Error traps are set for detecting if any internally generated expressions are "too large." If any traps are triggered, or if the resulting inert expression involves terms other than $Z[\,]$ or $Z[p]$ for p a prime integer, then the greedy method is designated as having "failed," and the algorithm restarts in conservative mode. In this mode, we examine every opportunity to apply (R2), but apply only one of them; namely, the one that produces the smallest results. If there is no opportunity to apply (R2), we do the same with (R1). Then the full algorithm is recursively applied to each of the new expressions (i.e., first greedy mode, and then if it fails, conservative mode) until an inert expression is reached.

B. Results.

In using this program to investigate the conjecture of Kontsevich, we were amazed at how effective it is at finding complete reductions. We had expected that it would be necessary to incorporate Buchberger-style reductions (e.g., $f_2 \to f_2 - af_1$, where a is chosen to kill the leading term of f_2), and perhaps invertible changes of variable, in order to obtain results for all but the smallest problems.

For example, the complete bipartite graph $K_{3,3}$ has 81 spanning trees, so $\Sigma(G)$ is a sum of 81 square-free monomials of degree 5 in 9 variables. It typically takes about 17 or 18 rounds in greedy mode to obtain a complete reduction that proves

$$Z[\Sigma(K_{3,3})](q) = q^{-1} + 7q^{-3} - 13q^{-4} + 14q^{-5} - 17q^{-6} + 9q^{-7}.$$

Due to the randomized nature of the algorithm, it is possible for the greedy mode to fail for this graph, thus creating the need for a round of conservative reduction. On the other hand, for slightly larger graphs, several rounds in conservative mode are often required.

Bearing in mind Corollaries 2.5 and 2.7, we searched for a minimal counterexample to Conjecture 2.1. We generated all connected graphs with no cut vertex (cf. (2.5)), no two-edge cutset, no triple of vertices satisfying $N(u) \subseteq N(v), N(v')$, and at most 13 edges. The number of such graphs, sorted by edge and vertex counts, is displayed in Table I.

For the graphs with $\leqslant$11 edges, and all but two of the graphs with 12 edges, the program was able to find a complete reduction of $\Sigma(G)$. The two exceptional graphs are the cubic graphs of girth four on eight vertices: the cube Q, and the "Möbius ladder" L—the graph obtained by adding edges joining the antipodal points of an eight-vertex circuit.

Since the cube is a planar graph, there is a natural bijection between the edges of Q and its planar dual, the octahedron O. Furthermore, this identification induces a bijection between the spanning trees of O and complements of spanning trees in Q (e.g., see Lemma 2.3.7 in [**O**]). In particular, $Z[\Sigma(O)] = Z[\bar{\Sigma}(Q)]$. However, included among the calculations mentioned above is a complete reduction for $\Sigma(O)$ (the octahedron has only six vertices), so it follows from Corollary 3.3 that $Z[\Sigma(Q)]$ must be a polynomial in q^{-1}.

Although the Möbius ladder is not planar, it is still an advantage that $\bar{\Sigma}(L)$ has degree five, whereas $\Sigma(L)$ has degree seven. We were able to obtain a complete reduction proving that $Z[\bar{\Sigma}(L)]$ is a polynomial in q^{-1}, so again it follows from Corollary 3.3 that $Z[\Sigma(L)]$ must be a polynomial in q^{-1}.

We conclude from these considerations that Kontsevich's conjecture is true for all graphs with at most 12 edges.

While we are skeptical that the following question has an affirmative answer, the unreasonable success of the algorithm prompts it.

QUESTION 5.1. *Is it true that $\Sigma(G)$ is completely reducible for every graph G?*

We have used the program to verify that this is true for all graphs with at most 11 edges. Note that we cannot use Corollary 2.5 to reduce the search to graphs with edge connectivity $\geqslant 3$, since the proof of Theorem 2.4 involves the use of Proposition 1.3 in the "reverse" direction. Similarly, we also cannot make use of Corollary 2.7.

A hint towards an explanation of the effectiveness of the algorithm is provided by Theorem 2.8. Recall that the quantity $\Delta_{e,e'}(G)$ appears when (R1) is applied twice to $Z[\Sigma(G)]$ (see Theorem 2.4). Since $\Delta_{e,e'}(G)$ is quadratic in each variable, it would be inert if it were irreducible. However Theorem 2.8 shows that $\Delta_{e,e'}(G)$ is a perfect square.

C. Interpolation.

Define the *depth* of the expression $q^{-d}Z[f_1,\ldots,f_k]$ to be $d+1$ if $[f_1,\ldots,f_k]$ is primitive, d if $[f_1,\ldots,f_k]$ is imprimitive but not identically zero, and infinite if $[f_1,\ldots,f_k]$ is zero (or an empty list). The depth of a $\mathbf{Z}$-linear combination of such expressions is defined to be the minimum depth of its constituents.

Note that $[\ ]$ and $[p]$ for prime integers p are the only imprimitive lists that are inert.

By Proposition 1.2, any expression of depth d is asymptotically $g_0(q^{-1}) + O(q^{-d})$ for some (explicit) polynomial g_0. Thus if our algorithm fails to completely reduce $\Sigma(G)$, instead producing an inert expression of depth d, then we will at least be able to determine an asymptotic series for $Z[\Sigma(G)](q)$ through terms of order less than q^{-d}.

Define the *embedding degree* of the expression $q^{-d}Z[f_1, \ldots, f_k]$ to be $m + d$, where m is the number of dependent variables that appear in $[f_1, \ldots, f_k]$. More generally, define the embedding degree of a $\mathbf{Z}$-linear combination of such expressions to be the maximum embedding degree of its constituents.

PROPOSITION 5.2. *Assume $f_1, \ldots, f_k$ are homogeneous of positive degree. If $g(q) = Z[f_1, \ldots, f_k](q)$ is a polynomial function of q^{-1}, then g can be explicitly determined from a reduction of $Z[f_1, \ldots, f_k]$ of depth d and embedding degree e, together with the values of $g(q)$ at $e - d$ prime powers q.*

Proof. Given the existence of a reduction as described, $q^e g(q)$ must be integer-valued for all prime powers q, so as a polynomial in q^{-1}, g has degree $\leqslant e$. Furthermore, since the reduction has depth d, one can extract from it an explicit polynomial g_0 such that

$$g(q) = g_0(q^{-1}) + a_d q^{-d} + a_{d+1} q^{-(d+1)} + \cdots + a_e q^{-e},$$

for certain (unknown) scalars $a_d, a_{d+1}, \ldots, a_e$. Now since $f_1, \ldots, f_k$ are homogeneous and nonconstant, it follows that the nonzero points on the corresponding variety can be partitioned into $\mathbf{F}_q^*$-orbits, each of size $q - 1$. Hence the polynomial $g(q)$ must evaluate to 1 at $q = 1$; i.e., $g_0(1) + a_d + \cdots + a_e = 1$, leaving a parameter space of dimension $e - d$. $\square$

REMARK 5.3. (a) As pointed out by Stanley (see Proposition 2.2 of [**St**]), the rationality of zeta functions of varieties over finite fields implies that the coefficients of $g(q)$ are necessarily integers. Thus if we use the interpolation suggested by the above proposition when $g(q)$ is not known in advance to be a polynomial, and it happens that the resulting coefficients are not integers, we obtain proof that $g(q)$ is not a polynomial.

(b) An expression of the form $Z[h_1, \ldots, h_l]$, where h_1 (say) is a nonzero integer, evaluates to 0 for infinitely many prime powers q. Thus in an application of Proposition 5.2, we may ignore such terms when computing the depth and embedding degree.

(c) If G has m edges and at least one cycle, then $Z[\Sigma(G)]$ has a reduction with embedding degree $\leqslant m - 1$. This follows by induction from Lemma 2.2, if we include graphs with loops or duplicate edges as part of the assertion, and take the basis of the induction to be graphs with at least one loop. In the latter case the result is obvious, since $\Sigma(G)$ depends on at most $m - 1$ variables.

As we mentioned previously, our program produced incomplete reductions for the cube and the Möbius ladder. For the cube Q, it produced a $\mathbf{Z}[q^{-1}]$-linear combination of $Z[\ ]$, $Z[2]$, and 13 inert expressions of the form $Z[f]$ for various polynomials f. The depth of the expression was 5 and the embedding degree 11, so since we do know that $Z[\Sigma(Q)]$ is a polynomial, we were able to determine it by explicitly counting points on the varieties $f = 0$ over the fields $\mathbf{F}_q$, $q = 2, 3, 4, 5, 7, 8$, obtaining

$$Z[\Sigma(Q)] = q^{-1} + 9q^{-3} + 3q^{-4} - 86q^{-5} + 191q^{-6} - 220q^{-7} + 133q^{-8} - 6q^{-9} - 24q^{-10}.$$

For redundancy, we also counted points over $\mathbf{F}_9$ and checked to see that it agreed with this result. As a further check of correctness, we also counted points on the variety $\Sigma(Q) = 0$ over $\mathbf{F}_2$ and $\mathbf{F}_3$ and compared it with this formula.

For the Möbius ladder L, our program produced a $\mathbf{Z}[q^{-1}]$-linear combination of $Z[\ ]$, $Z[2]$, $Z[3]$, and 137 inert expressions involving one, two, or three polynomials and scalars, the depth being 4 and the embedding degree 11. Proceeding as above, we needed one more evaluation than in the case of the cube, and used the count for $\mathbf{F}_{11}$ as a redundancy check. In this case, we obtained

$$Z[\Sigma(L)] = q^{-1} + 9q^{-3} + q^{-4} - 85q^{-5} + 203q^{-6} - 258q^{-7} + 176q^{-8} - 14q^{-9} - 32q^{-10}.$$

As before, we also counted solutions of $\Sigma(L) = 0$ over $\mathbf{F}_2$ and $\mathbf{F}_3$ and verified that the counts were consistent with this formula.

6. The Apex Case

As noted by Stanley in [**St**], the conjecture of Kontsevich is particularly interesting when the graph G has an *apex*—a vertex v that is adjacent to every other vertex. In that case, if we make a change of variables $x_e \to -x_e$ for all edges e not incident to v, then $\bar{L}_{v,v}(G)$ is a symmetric matrix whose entries are either zero (in certain off-diagonal positions) or independent indeterminates, aside from the symmetry condition.

Reformulating this slightly, given a simple graph G, let us define $M(G)$ to be the matrix whose rows and columns are indexed by the vertices of G, with the (u, v)-entry being x_{uv} (if $u \neq v$ and $uv = vu$ is an edge of G), or x_u (if $u = v$), or 0 (if u and v are non-adjacent). Considering (2.7), we have

$$Z[\Sigma(G^*)] = Z[\det M(G)],$$

where G^* denotes the graph obtained from G by adjoining a new vertex adjacent to all vertices of G. Thus the following is a special case of Conjecture 2.1.

Conjecture 6.1. *For all graphs G, $Z[\det M(G)]$ is a polynomial function of q^{-1}.*

Given a subset S of the edge set of G, let $M(G)|_S$ denote the matrix obtained from $M(G)$ by specializing $x_e = 1$ for all $e \in S$.

Theorem 6.2. *If G is a minimal counterexample to Conjecture 6.1, then*

(a) *G is connected.*

(b) *Every vertex of G has degree $\geqslant 2$.*

(c) *There is no pair of vertices u, v such that $N(u) \subseteq N(v)$.*

(d) *For all acyclic subgraphs T of G, $Z[\det M(G)|_T]$ is not a polynomial in q^{-1}.*

Proof. (a) If G is disconnected, then $\det M(G) = \det M(G_1) \det M(G_2)$ for certain subgraphs G_1 and G_2, and hence (cf. (2.2))

$$Z[\det M(G)] = Z[\det M(G_1)] + Z[\det M(G_2)] - Z[\det M(G_1)] \cdot Z[\det M(G_2)].$$

(b) If v has degree 1 in G, then it has degree 2 in G^*. Hence the two edges e, e' incident to v form a minimal cutset in G^*. (Given that G is connected and has more than two vertices, all doubleton edge cuts in G^* are of this form.) Applying (2.5) to G^*, we obtain that $Z[\det M(G)]$ is a $\mathbf{Z}[q^{-1}]$-linear combination of expressions of the form $Z[\det M(G')]$ for three smaller graphs G', contradicting the minimality of G.

(c) Suppose $N(u) \subseteq N(v')$. Adjoining an apex v, the same relationship holds in G^*. Since u has degree at least two in G, there must be another vertex u' in G adjacent to u (and hence also v'). Hence the identity of Theorem 2.6 applies to G^*. Since each of the constituent graphs of this identity have v as an apex, we contradict the minimality of G.

(d) By inclusion-exclusion, the quantity

$$P(q) = P_{G,T}(q) := \sum_{S \subseteq T} (-q)^{-|S|} Z[\det M(G - S)](q)$$

represents the probability that a randomly chosen evaluation of the matrix $M(G)$ in $\mathbf{F}_q$ is singular and has nonzero entries in each of the positions indexed by T. Furthermore, since G is minimal, the expression $Z[\det M(G - S)](q)$ is a polynomial if and only if $S \neq \emptyset$, so $P(q)$ cannot be a polynomial function of q^{-1}.

Now choose a root vertex for each connected component of T, and let $\mathcal{D}(q)$ denote the group of (invertible) diagonal matrices D over $\mathbf{F}_q$ such that $D_{v,v} = 1$ unless v is an unrooted vertex of T. Note that $\mathcal{D}(q)$ acts on the set of singular evaluations of $M(G)$ over $\mathbf{F}_q$ via $M \mapsto DMD$, and this action preserves the zeroes of the matrix. Furthermore, it is not hard to show that an evaluation of $M(G)$ with nonzero entries in the positions of T has a trivial $\mathcal{D}(q)$-stabilizer; thus the singular matrices of this form can be partitioned into $\mathcal{D}(q)$-orbits each of size $(q-1)^{|T|}$, and the matrices with 1's in the positions indexed by T serve as orbit representatives. It follows that

$$P(q) = (1 - q^{-1})^{|T|} Z[\det M(G)|_T](q),$$

whence $Z[\det M(G)|_T]$ cannot be a polynomial in q^{-1}. $\square$

	4	5	6	7	8	9	10	11	12
4	1								
5		1	1						
6			1	2	3	2			1
7				1	4	9	11	7	6
8					1	7	26	53	80
9						1	10	56	200
10							1	14	121
11								1	19
12									1

TABLE II. Potential counterexamples to Conjecture 6.1.

REMARK 6.3. In the proof of (d), it would be natural to try to use the action of the full group of diagonal matrices. However the orbit structure is much more complicated, and the characteristic 2 case is exceptional. On the other hand, it can be shown that there is an analogue of (d) in which we permit T to have a unique cycle, provided that this cycle has odd length. (This is possible if and only if G is not bipartite.) In this case, one uses the action of $\mathbf{F}_q^* \times \mathcal{D}(q)$, the first factor acting via scalar multiplication.

We investigated Conjecture 6.1 by first generating all graphs with at most 12 edges that meet conditions (a)–(c) of Theorem 6.2. The number of such graphs, sorted by edge and vertex counts, is displayed in Table II. Remember that if there are n vertices and m edges, this represents an instance of Conjecture 2.1 with $m + n$ edges, so these are substantially larger problems than those listed in Table I.

We then used the *Maple* program described in §5 to reduce $\det M(G)|_T$ for a randomly chosen spanning tree T (for smaller graphs, we reduced $\det M(G)$ itself). For every graph with $\leqslant 11$ edges, we obtained a complete reduction, so we conclude that Conjecture 6.1 is true for all graphs with $\leqslant 11$ edges. We also checked the 12-edge graphs with $\leqslant 7$ vertices, and a few of the graphs with 8 vertices. In every case we obtained a complete reduction.

7. Related Questions

There are a number of natural variations and generalizations of Kontsevich's conjecture that turn out to be false.

A. Non-symmetric determinants.

For example (see [**St**]), consider dropping the symmetry condition in Conjecture 6.1. Equivalently, suppose we have a bipartite graph G on $n+n$ vertices (i.e., n vertices in each color class). Define $A(G)$ to be the $n \times n$ matrix with rows and columns indexed by the two colors of vertices, the (u, v)-entry being x_{uv} if uv is an edge of G, and 0 otherwise.

Question 7.1. *Is $Z[\det A(G)]$ a polynomial in q^{-1} for all G?*

Kontsevich suggested in a message to Stanley that a negative answer to this question follows from the non-representability of the Fano plane over fields of characteristic $\neq 2$. In fact, taking G to be the point-line incidence graph of the Fano plane (a regular bipartite graph with 21 edges and $7+7$ vertices), we used the program in §5 to determine that

$$1 - Z[\det A(G)] = (1-q^{-1})^7 g(q^{-1}) - q^{-5}(1-q^{-1})^{13} Z[2],$$

where

$$g(q) = 1 + 6q + 20q^2 + 35q^3 - 7q^4 - 97q^5 + 120q^6 - 74q^7 + 16q^8 + 9q^9 - 6q^{10} + q^{11},$$

thus confirming that Question 7.1 has a negative answer.

We also conducted a search to determine whether the incidence graph of the Fano plane is the smallest graph G such that $Z[\det A(G)]$ is not a polynomial. Considering that there are 2310376 bipartite graphs with 21 edges and $7+7$ vertices (up to color-preserving isomorphism), this search space requires pruning.

Theorem 7.2. *If G is a minimal bipartite graph such that $Z[\det A(G)]$ is not a polynomial function of q^{-1}, then*

(a) *G is connected.*
(b) *Every edge of G participates in a perfect matching.*
(c) *For all acyclic subgraphs T of G, $Z[\det A(G)|_T]$ is not a polynomial in q^{-1}.*
(d) *There are no vertices u, u' such that $\bar{N}(u) \subseteq \bar{N}(u')$, where $\bar{N}(u) := N(u) - \{u\}$.*
(e) *For every edge $e = uv$, there are at least $|\bar{N}(u)|$ non-adjacent pairs (u', v') with $u' \in \bar{N}(v)$ and $v' \in \bar{N}(u)$.*
(f) *Every vertex has degree $\geqslant 3$.*
(g) *Every vertex is non-adjacent to at least two vertices of the opposite color.*

Proof. (a) Similar to the proof of Theorem 6.2(a).

(b) If there are no perfect matchings of G that contain the edge e, then $\det A(G)$ does not depend on x_e and e can be deleted.

(c) Choose a root vertex for each connected component of T, and follow the proof of Theorem 6.2(d). The only necessary change is that one should employ the group action $A \mapsto D_1 A D_2$, where D_1, D_2 range over diagonal matrices supported on the unrooted vertices of T belonging to the two color classes.

(d) Suppose $\bar{N}(u) \subseteq \bar{N}(u')$. Since G is connected, there is some vertex v adjacent to u (and hence also u'). Since the columns in row u that have variable entries are a subset of those in row u', it follows by reasoning similar to the proof of Theorem 2.6 that $\det A(G)|_T$ and $\det A(G-u'v)|_T$ have the same distribution over $\mathbf{F}_q$, where $T=\{uv\}$. Hence

$$Z[\det A(G)|_T] = Z[\det A(G-u'v)|_T].$$

On the other hand, we know that

$$Z[\det A(G-u'v)|_T] = Z[\det A(G-u'v)] - q^{-1}Z[\det A(G-uv-u'v)]$$

is a polynomial since G is minimal, so this contradicts (c).

(e) We may assume that u (and similarly v) is adjacent to additional vertices. Otherwise, we violate (a), or (b), or G consists of the single edge uv. For each vertex $v' \in \bar{N}(u)$ other than v, there must be at least one vertex in $\bar{N}(v)$ that is not adjacent to v' (by (d)), so there are at least $|\bar{N}(u)|-1$ non-adjacent pairs in $\bar{N}(v)\times\bar{N}(u)$.

Thus if (e) is violated, there must be exactly one member of $\bar{N}(v)$ that is non-adjacent to each v', and we have a configuration of entries in $A(G)$ such as the following:

$$\begin{array}{ccccc} & v & v' & v'' & v''' \\ u & x_{11} & x_{12} & x_{13} & x_{14} \\ u' & x_{21} & x_{22} & x_{23} & 0 \\ u'' & x_{31} & 0 & 0 & x_{34}. \end{array}$$

Here we are supposing that $\bar{N}(u)=\{v,v',v'',v'''\}$ and $\bar{N}(v)=\{u,u',u''\}$, so that row u and column v are zero in $A(G)$ outside of this submatrix. The crucial point is that there is exactly one zero in each column of the submatrix beyond the first.

Set $T=\{u'v : u'\in\bar{N}(v)\}$ and consider $A(G)|_T$. In the above example, this amounts to setting $x_{11}=x_{21}=x_{31}=1$. If we now add multiples of column v of $A(G)|_T$ to the columns of $\bar{N}(u)$ so as to kill the nonzero entries of row u, the net effect is that the 0 in column v' of the submatrix becomes $-x_{uv'}$. In the above example, the variables x_{12}, x_{13}, x_{14} move to the positions currently occupied by 0's (and change sign). The new matrix again has entries that are, aside from 0's and 1's, independently and uniformly distributed over $\mathbf{F}_q$. We conclude that $\det A(G)|_T$ and $\det A(G')|_T$ have the same distribution, where G' is obtained from G by adding edges between every pair $(u',v')\in\bar{N}(v)\times\bar{N}(u)$, and deleting all edges incident to u other than the edge uv.

The new graph G' has the same number of edges as G, but it has edges $u'v : u'\in\bar{N}(v)$ that cannot appear in a perfect matching, so $Z[\det A(G')]$ must be a polynomial in q^{-1}, and the same must be true for all subgraphs of G'. By an inclusion-exclusion argument similar to the proof of Theorem 6.2(d), it follows that

$$Z[\det A(G)|_T] = Z[\det A(G')|_T] = P(q^{-1})/(1-q^{-1})^{|T|}$$

for some polynomial P. This is possible only if $Z[\det A(G)|_T]$ is itself a polynomial in q^{-1}, contradicting (c).

(f) If v has degree 2 and u is a vertex of degree $k \geqslant 2$ adjacent to v, then (e) implies that there can be at most k edges between $\bar{N}(v)$ and $\bar{N}(u)$. However, we have already accounted for $k+1$ such edges.

(g) We know that every vertex must be non-adjacent to at least one vertex of the opposite color (by (d)), so if (g) is violated, there must be a vertex u that is non-adjacent to a unique vertex v of the opposite color. Furthermore, again by (d), u must also be the unique vertex of the opposite color that is non-adjacent to v.

There are at least two other (in fact by (f), three other) vertices u', u'' of the same color as u. Since their neighborhoods must be incomparable, there exist edges $u'v'$ and $u''v''$ in G such that (u', v'') and (u'', v') are non-adjacent pairs. Thus in $A(G)$ we have a submatrix of the form

$$\begin{array}{cccc} & v & v' & v'' \\ u & 0 & x_{12} & x_{13} \\ u' & x_{21} & x_{22} & 0 \\ u'' & x_{31} & 0 & x_{33}, \end{array}$$

and the remaining entries in row u and column v are variables.

Now set $T = \{u'v, u''v, u'v', u''v''\}$ and consider $A(G)|_T$; i.e., $x_{21}, x_{31}, x_{22}, x_{33} = 1$. Subtracting multiples of rows u' and u'' from row u to kill the (u, v')- and (u, v'')-entries, we obtain a new matrix whose (u, v)-entry is $-x_{12} - x_{13}$, and aside from 0's and 1's, the entries are independently and uniformly distributed over $\mathbf{F}_q$. We conclude that $\det A(G)|_T$ and $\det A(G')|_T$ have the same distribution, where G' is obtained by adding uv and deleting uv' and uv'' from G. We now obtain a contradiction by reasoning similar to (e). $\square$

There are no graphs satisfying the conditions of Theorem 7.2 with less than 6+6 vertices. For example, with $5+5$ vertices, (f) and (g) force the graph to be cubic. There are only two such graphs, their (bipartite) complements being a 10-cycle and the union of a 4-cycle and a 6-cycle. The latter violates (d), whereas the former violates (e).

Omitting (c), there are 6 graphs on $6+6$ vertices that meet the conditions of Theorem 7.2—one each with 18, 19, 20, and 21 edges, and two with 24. For each of these graphs, we chose a spanning tree T and used the program described in §5 to obtain a complete reduction of $\det A(G)|_T$, thereby proving that there are no examples on $6+6$ vertices.

For graphs on $7+7$ vertices, the minimum possible number of edges is 21, by (f). There are three graphs with 21 edges that meet all of the above conditions (other than (c)), and we found that only the incidence graph of the Fano plane has a spanning tree specialization that fails to produce a polynomial. It follows that this is the only graph with $\leqslant 21$ edges such that $Z[\det A(G)]$ is not a polynomial in q^{-1}.

B. Matroids.

Generalizing from graphs to matroids, it is natural to define $\Sigma(M)$ to be the generating function for the bases of a matroid M. The original formulation of Kontsevich's conjecture in terms of complements of spanning trees is the statement that if M is a co-graphic matroid, then the number of zeroes of $\Sigma(M)$ over $\mathbf{F}_q$ should be a polynomial in q.

If we consider the matroid M_n of an n-point line, then every pair of points forms a base, and $\Sigma(M_n) = \sum_{i<j} x_i x_j$. However, as pointed out by Stanley in [**St**], the number of zeroes of $\Sigma(M_4)$ over $\mathbf{F}_q$ is not a polynomial in q. Indeed, using only two rounds of reductions, one obtains

$$Z[\Sigma(M_4)] = q^{-1} - q^{-2} + q^{-1} Z[x^2 + xy + y^2].$$

One can show that this is not a polynomial by analyzing when $x^2 + xy + y^2$ is irreducible or a perfect square (or neither) over $\mathbf{F}_q$. Or use the methods of §5C.

On the other hand, both Tim Chow and Alexander Barvinok have suggested restricting to the class of regular (or unimodular) matroids. These are the linear matroids that are representable over every field, and can roughly be described as the class of matroids for which one has an analogue of the Matrix-Tree Theorem.

The smallest[3] regular matroid that is neither graphic nor co-graphic, labeled R_{10} in [**O**], can be represented over every field by the matrix

$$L = \begin{bmatrix} -1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

In other words, the bases of R_{10} are the sets of columns of nonzero maximal minors of L, and since this is a universal representation of R_{10}, these nonzero minors are all ± 1. By the analogue of the Matrix-Tree Theorem (a Binet-Cauchy expansion), one has

$$\Sigma(R_{10}) = \det LDL^t,$$

where D is a diagonal matrix of indeterminates.

We applied the reduction algorithm to $\Sigma(R_{10})$, obtaining

$$\begin{aligned} Z[\Sigma(R_{10})] = {} & q^{-1} + q^{-3} + 15q^{-4} - 27q^{-5} + 4q^{-6} + 8q^{-7} \\ & + (q^{-6} - q^{-7})(7Z[2] + 3Z[3]) - q^{-3} Z[f], \end{aligned}$$

[3] In terms of the ground set, which in the case of a graph is the number of edges.

where f is an irreducible, primitive polynomial in 5 variables. This expression has depth 4 and embedding degree 8, so if we accept the hypothesis that $Z[\Sigma(R_{10})](q)$ is a polynomial in q^{-1}, then it can be explicitly determined by evaluating the above expression at four prime powers q (Proposition 5.2).

We counted the zeroes of f over $\mathbf{F}_q$, $q = 2, 3, 4, 5$, and found that the unique polynomial that fit the data did not have integer coefficients. Hence (see Remark 5.3(a)), $Z[\Sigma(R_{10})]$ cannot be a polynomial in q^{-1}. (Alternatively, one can count zeroes of f over $\mathbf{F}_7$ and see that the result does not fit the polynomial.) As a check, we also counted the zeroes of $\Sigma(R_{10})$ over $\mathbf{F}_2$ and $\mathbf{F}_3$, and confirmed that it agreed with the above formula and data.

Thus even for regular matroids, the analogue of Kontsevich's conjecture fails.

References

[**C**] T. Chow, private communication.

[**D**] C. L. Dodgson, Condensation of determinants, *Proc. Roy. Soc. London* **15** (1866), 150–155.

[**L**] L. Lovász, "Combinatorial Problems and Exercises," North-Holland, Amsterdam, 1979.

[**O**] J. G. Oxley, "Matroid Theory," Oxford University Press, New York, 1992.

[**St**] R. P. Stanley, Spanning trees and a conjecture of Kontsevich, preprint.

[**Z**] D. Zeilberger, Dodgson's determinant-evaluation rule proved by two-timing men and women, *Electron. J. Combin.* **4** (2) R22 (1997), 2pp.