ELEMENTARY APPLICATIONS OF A TECHNICAL THEOREM

BRIAN OSSERMAN

Abstract. Mochizuki proves a technical theorem concerning the stack of "dormant torally indigenous bundles" over the stack of stable curves; without saying anything about what these bundles are, we give two elementary applications of this result, the first (joint with Fu Liu) to counting lattice points inside polytopes, and the second to rational functions with prescribed ramification in positive characteristic. The combinatorial application is notable in that the particular bundles in question are completely irrelevant, and the result potentially provides a template for a variety of similar applications of algebraic geometry to combinatorics.

1. A Finite-flatness Result

This talk is based upon [1] and [2]; see these for details.

We begin by stating a highly technical result of Mochizuki. We assume throughout that we are working over an algebraically closed field of characteristic $p > 2$. If C is a nodal curve with marked points, we denote its normalization by $\tilde{C}$, and adopt the convention that its marked points are the points lying above marked points or nodes of C. We call those curves parametrized by $\overline{\mathcal{M}}_{g,r}$ **curves of type** (g, r): nodal, proper curves C of genus g with r marked points, such that each component of $\tilde{C}$ having genus 0 has at least 3 marked points, and each component of genus 1 has at least 1 marked point. Finally, a **totally degenerate** curve C is one such that $\tilde{C}$ consists entirely of genus 0 curves with exactly three marked points.

Theorem 1.1. *(Mochizuki) Given (g, r) with $2g-2+r > 0$, and radii $\rho_1, \dots, \rho_r \in \mathbb{F}_p/\pm 1$, the stack of dormant torally indigenous bundles (DTIBs) of radii $\{\rho_i\}$ on curves of type (g, r) is finite and flat over $\overline{\mathcal{M}}_{g,r}$.*

Furthermore, over any totally degenerate curve C, the stack of DTIBs is étale, and the number of DTIBs is given as the number of ways of assigning odd integers between 0 and p to each of the marked points of $\tilde{C}$, such that marked points gluing to give a node of C are assigned the same integer, and on each component of $\tilde{C}$ the three integers satisfy the triangle inequality, and have sum less than $2p$. The integers assigned to points lying over marked points are the unique odd representatives of the radii at the points.

What DTIBs actually are will not be relevant to our talk; all that matters is that they are objects which can be associated to any curve of type (g, r), with "radii" at each marked point in $\mathbb{F}_p/\pm 1$. The theorem asserts that on any curve there are only finitely many DTIBs, that the number on a general curve may be computed as the number on any totally degenerate curve, and that for any totally degenerate curve there is a combinatorial formula for this number. For the curious, DTIBs are defined as certain $\mathbb{P}^1$-bundles with section and connection on the curve in question, and are related to Frobenius-destablized vector bundles of rank 2.

We will give two different types of applications; the first doesn't require knowing anything more about DTIBs, while the second will require the following theorem in the case $g = 0$ (the $r = 3$ case was previously shown by Mochizuki):

Theorem 1.2. *Fix radii* $\{\rho_i\}$ *for each of the* r *marked points on* $C = \mathbb{P}^1$, *with sign mod* p *chosen so that* $0 < \rho_i < \frac{p}{2}$. *Then there is a natural map* φ *from the set of self-maps of* $\mathbb{P}^1$ *ramified to order* $p - 2\rho_i$ *at the marked points and unramified elsewhere, to the set of dormant torally indigenous bundles on* $\mathbb{P}^1$ *of radii* $\{\rho_i\}$. *We have further:*

(i) *The map* φ *is injective after passing to equivalence classes of maps related by post-composition by automorphisms of the image.*
(ii) *If the marked points are general, the map* φ *is surjective.*
(iii) *If the marked points are general, there is a bijective correspondence between self-maps of* $\mathbb{P}^1$ *as above, and self-maps of* $\mathbb{P}^1$ *for which any even number of the ramification indices* $p - 2\rho_i$ *have been replaced by* $2\rho_i$.

We make some general remarks on how the second part of Theorem 1.1 arises, since it is in fact very natural. Indeed, one need only know two additional facts. The first fact is then that DTIBs can be glued as long as radii agree: specifically, given a nodal curve C, a DTIB on C with given radii is equivalent to a DTIB on $\widetilde{C}$ with the same radii at marked points lying above marked points of C, and arbitrary radii at the marked points lying above nodes, subject to the constraint that the radii at the two points above a node must agree. The second fact is that in the case of three ramification points on $\mathbb{P}^1$, given odd ramification indices e_i less than p, at most one map exists with that ramification, and existence is equivalent to the conditions that the e_i satisfy the triangle inequality and have sum less than $2p$, (which is fairly natural, since these may be rephrased as saying that each e_i can be at most the degree of the map, and the degree should be less than p, respectively). Neither fact is hard to prove, and together with the $r = 3$ case of Theorem 1.2 they immediately yield the second statement of the theorem.

2. A Combinatorial Application

We first describe an application of Theorem 1.1 to combinatorics, developed in joint work with Fu Liu. This is notable mainly because it requires no knowledge whatsoever of what DTIBs are, and indeed relies only on formal properties that one might expect to come up fairly frequently in enumerative geometry. The basic observation is as follows: as noted earlier, Mochizuki's theorem means that the number of DTIBs on a general curve of type (g, r) is given by any of the combinatorial formulas corresponding to totally degenerate curves of the same type. Since there are multiple totally degenerate curves of any given type, one obtains identities between all the different combinatorial formulas. Since this involves only the general situation of finite-flatness over $\overline{\mathcal{M}}_{g,r}$, and étaleness and combinatorial formulas at totally degenerate curves, it seems this ought to occur naturally in a variety of scenarios. However, we will briefly explore the specific form these identities take in our case of DTIBs. In order to do so, we need to make some preliminary definitions.

Definition 2.1. Let V, E be sets, and suppose that we are given φ a map from E to $V \cup \left(\binom{V}{2}\right)$. We then call $G = (V, E, \varphi)$ a **quasi-graph**. The standard notions of **edges**, **vertices**, and edges being **adjacent** to vertices generalize immediately to quasi-graphs. The set of edges E is naturally subdivided into **free** edges, which are $\varphi^{-1}(V)$, and **fixed** edges, given by $\varphi^{-1}\left(\binom{V}{2}\right)$.

Thus, a quasi-graph may be thought of simply as a graph where some edges – the free edges – are allowed to be attached to only a single vertex. A quasi-graph which consists of only fixed edges is simply a standard graph. Quasi-graphs arise naturally as the dual objects to nodal curves with marked points: we define the **dual quasi-graph** to have a vertex for each component of the curve, a fixed edge for each node, and a free edge for each marked point. A quasi-graph is said to be **regular** of degree m if there are m edges adjacent to each vertex, counting loops with multiplicity 2.

Recall that a convex polytope is defined to be the convex hull of a set of points in some $\mathbb{R}^n$, or equivalently, a bounded intersection of half-spaces.

Definition 2.2. Let G be a quasi-graph which is regular of degree 3. The convex polytope $\mathscr{P}_G$ associated to G is defined to be the space of real-valued weight functions $w : E \to \mathbb{R}$ on the edge set of G satisfying the following inequalities:

(i) for each $e \in E$, $w(e) \geq 0$;
(ii) for each $v \in V$, $\sum_{e\in A(v)} w(e) \leq 1$;
(iii) for each $v \in V$ and $e \in A(v)$, $w(e) \leq \sum_{e' \in A(v) \smallsetminus \{e\}} w(e')$.

Here $A(v)$ denotes the set edges adjacent to each vertex, with multiplicity in the case of loops.

Note that condition (iii) is just the triangle inequality for the edges adjacent to any given vertex. Note also that (i) and (ii) bound all the $w(e)$ between 0 and 1, so in particular $\mathscr{P}_G$ is in fact a polytope.

Our combinatorial result will then take the form of identities between the number of lattice points of scalings of the $\mathscr{P}_G$ for different G. Before we describe this, we state a general combinatorial theorem on lattice points of rational polytopes:

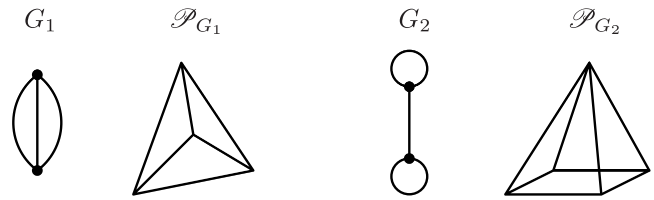
Theorem 2.3. *(Ehrhart) Let $\mathscr{P}$ be a rational polytope: i.e., a polytope with vertices having rational coordinates. Suppose that the least common denominator of the vertices is d. For $n \in \mathbb{Z}_{\geq 0}$, denote by $n\mathscr{P}$ the polytope obtained by scaling $\mathscr{P}$ by a factor of n. Then there exist polynomials $f_0, \dots, f_{d-1}$ such that the number of lattice points in $n\mathscr{P}$ is given by $f_i(n)$, where $i \equiv n \pmod{d}$. In particular, if $\mathscr{P}$ has integral vertices, the number of lattice points in $n\mathscr{P}$ is given by a single polynomial in n.*

Thus, the function giving the number of lattice points in $n\mathscr{P}$ is called the **Ehrhart quasi-polynomial** of $\mathscr{P}$. Not very much is known about Ehrhart polynomials. Their degree is the dimension of the polytope, their leading coefficient the volume, and the second coefficient has a similar description. However, the other coefficients remain mysterious.

We can now state the combinatorial result:

Theorem 2.4. *(Liu-Osserman) Let G, G' be any two quasi-graphs, connected, regular of degree three, and having the same number of vertices and edges. Then the Ehrhart quasi-polynomials for $\mathscr{P}_G$ and $\mathscr{P}_{G'}$ agree at all odd values.*

Given Mochizuki's results, the proof of this result is rather straightforward. One first shows that the least common denominator of the vertices of $\mathscr{P}_G$ always divides



The case $(g, r) = (2, 0)$

4, and then we can apply Mochizuki's results with $n = p - 2$ as p varies over odd primes to obtain the desired results for $p \equiv 1, 3 \pmod 4$.

Example 2.5. Consider the case of $(g, r) = (2, 0)$, or equivalently graphs with three edges and two vertices. One checks that we get only two graphs: the G_1 and G_2 of the figure. The corresponding polytopes $\mathscr{P}_{G_1}$ and $\mathscr{P}_{G_2}$ are, respectively: a regular tetrahedron with vertices at $(0,0,0)$, $(\frac{1}{2}, \frac{1}{2}, 0)$, $(0, \frac{1}{2}, \frac{1}{2})$ and $(\frac{1}{2}, 0, \frac{1}{2})$; and a square pyramid with vertices $(0,0,0)$, $(\frac{1}{2}, 0, 0)$, $(0, \frac{1}{2}, 0)$, $(\frac{1}{2}, \frac{1}{2}, 0)$ and $(\frac{1}{4}, \frac{1}{4}, \frac{1}{2})$. One finds that in fact not only the odd values, but the entire Ehrhart quasi-polynomials of $\mathscr{P}_{G_1}$ and $\mathscr{P}_{G_2}$ agree, and are given by $\frac{1}{24}(n^3 + 6n^2 + 20n + 24)$ for even n and $\frac{1}{24}(n^3+6n^2+11n+6)$ for odd n. The number of dormant torally indigenous bundles in this case is thus given by $\frac{1}{24}(p^3 - p)$.

3. Applications to Rational Functions with Prescribed Ramification

We next use Theorem 1.2 to apply Theorem 1.1 to rational functions with prescribed ramifications. In fact, one may take the results of the previous section further, showing that the odd values of the Ehrhart-quasipolynomial of $\mathscr{P}_G$, and hence DTIBs, are counted by a single polynomial. Restricting to $g = 0$ and using Theorem 1.2, the strongest statement we can conclude is the following.

Theorem 3.1. *(Liu-Osserman) Given r general marked points on $\mathbb{P}^1$, the number of maps $f : C = \mathbb{P}^1 \to \mathbb{P}^1$ ramified to order less than p at the marked points and unramified elsewhere, counted modulo automorphism of the image, is given by $f_r(p)$, where $f_r(n)$ is a polynomial in $\mathbb{Q}[n]$ of degree $2r - 3$, is even or odd depending on its degree, and is strictly positive for $n \geq 2$.*

Indeed, we also find that we have a formula for the number of maps with prescribed ramification. Specifically, the following theorem follows fairly immediately from Theorems 1.1 and 1.2.

Theorem 3.2. *Given d, n and $e_1, \ldots, e_n$ with $e_i < p$ and $e_i \leq d$ for all i and $2d - 2 = \sum_i (e_i - 1)$, the number $N_{\text{gen}}(\{e_i\}_i)$ of separable self-maps of $\mathbb{P}^1$ of degree d and ramified to order e_i at general P_i, modulo automorphism of the image space, is given as the number of ways of inserting $n-2$ indices e'_j into the sequence $e_1, \ldots, e_n$, starting after e_2 and alternating thereafter, such that the following condition is satisfied: if e, e', e'' is any consecutive triple of the newly obtained sequence which starts on in an odd place in the sequence (i.e., $e = e_1$ or e'_j for some j), then e, e', e'' satisfies the triangle inequality, and we further have that $e + e' + e''$ is odd and less than $2p + 1$.*

This replicates (and in fact precedes and provides motivation for) the direct argument for an equivalent formula given in [3]. In essence, Theorem 1.1 is used to bypass the need for a result controlling when separable maps can degenerate to inseparable maps, and can in fact be used to conclude such a result. However, because we do have a self-contained argument for this theorem, it also follows that we could prove Theorem 3.1 without any reference to Mochizuki's work. But there is one result on rational functions which at present does require the application of Mochizuki's results.

Theorem 3.3. *Fix distinct points $P_1, \dots, P_r$ on $\mathbb{P}^1$, and odd integers $e_1, \dots, e_r$ less than p. Then the number of maps from $\mathbb{P}^1$ to itself which are ramified to order e_i at the P_i and unramified elsewhere, when counted modulo automorphisms of the image $\mathbb{P}^1$, is finite.*

This is actually the simplest application so far, following immediately from the finiteness statement of Theorem 1.1 together with the injectivity assertion of Theorem 1.2 (i).

We make several remarks on this result. First, the restriction to odd e_i is strongly expected to be unnecessary, and could almost certainly be removed via a generalization of the construction leading to Theorem 1.2, following Mochizuki's approach in the case $r = 3$. In contrast, the restriction to $e_i < p$ is absolutely essential, as demonstrated by the family of (tamely ramified) rational functions $x^{p+2} + tx^p + x$. Finally, unlike the situation with the earlier two Theorems, a direct argument for this result is not known and does not appear to be on the horizon. The main issue is that the finiteness of Theorem 1.1 is proved by considering a larger class of objects than than DTIBs (replacing a vanishing p-curvature hypothesis by nilpotent p-curvature) and first proving finite-flatness in that setting. There is no apparent way to translate this enlarged class into the setting of rational functions with prescribed ramification.

We conclude by discussing an application of our finiteness theorem to the theory of branched covers, where one specifies the points on the base over which the ramification should occur, rather than the ramification points on the source curve. Theorem 3.2 gives in particular precise criteria for when a map from $\mathbb{P}^1$ to $\mathbb{P}^1$ can exist with particular ramification indices less than p, when the ramification points are general. *A priori*, there is no way to rule out the possibility that for some choice of e_i, such maps do not exist for general P_i, but do exist in higher-dimensional families for special configurations of P_i, and hence exist for general configurations of branch points. That is indeed exactly what happens for the aforementioned family $x^{p+2} + tx^p + x$; although the ramification points remain fixed as t varies, their images move. However, the finiteness result rules out this behavior for $e_i < p$, and in fact leads to the stronger result that maps existing for general ramification points is equivalent to them existing for general branch points is equivalent to them existing at all. In particular, we can produce a broad class of examples of branched covers of $\mathbb{P}^1$ by $\mathbb{P}^1$ which exist in characteristic 0, but don't exist in characteristic p. Although there are various partial existence results in positive characteristic, I am not aware of any prior substantial non-existence results.

References

1. Fu Liu and Brian Osserman, *Mochizuki's indigenous bundles and Ehrhart polynomials*, Journal of Algebraic Combinatorics **23** (2006), no. 2, 125–136.
2. Brian Osserman, *Mochizuki's crys-stable bundles: A lexicon and applications*, Publications of RIMS, to appear.

3. ———, *Rational functions with given ramification in characteristic p*, Compositio Mathematica **142** (2006), no. 2, 433–450.