COMBINATORIAL INTERPRETATIONS OF THE TRACE MOMENT SEQUENCES OF SUBGROUPS OF $USp(4)$

DHROOVA AIYLAM, CARLOS CORTEZ
X MENTOR : DAVID CORWIN

SPUR Final Paper, Summer 2014
Projected suggested by: Prof. Drew Sutherland

Abstract. Fité et al. (2011) describe a generalization of the Sato-Tate conjecture by hypothesizing that the distribution as p varies, for a fixed algebraic curve, of the normalized error terms $((p+1-\text{number of solutions})/g\sqrt{p})$ follows the distribution of the trace of a random element of some subgroup of $USp(2g)$, called the Sato-Tate group of the curve. In genus two, there are 55 non-isomorphic possibilities for the Sato-Tate group, although some have the same trace moment sequence. When the group is connected, the work of Magyar and Grabiner shows that these kind of sequences can be naturally interpreted as counting certain walks over a lattice of dimension g when working in general with subgroups of $USp(2g)$. In this paper, we look at what kinds of combinatorial problems arise from the trace moment sequences of the not necessarily connected Sato-Tate groups, and how they relate to the component group in these disconnected cases.

1. Introduction

1.1. Elliptic Curves

We begin with a brief discussion of elliptic curves - for our purposes, curves of the form $y^2 = f(x)$ with $f(x) = x^3 + ax + b$ for some $a, b \in \mathbb{Q}$.

Definition 1.1. *We say an elliptic curve is* non-singular *if the partial derivatives of,* $\frac{\partial f}{\partial x}, \frac{\partial y^2}{\partial y} = 2y$ *never vanish simultaneously; equivalently, if the* discriminant $\Delta = -16(4a^3 + 27b^2)$ *is non-zero in* $\mathbb{Q}$.

Definition 1.2. *A* projective solution *to an elliptic curve is a triple* $(X, Y, Z) \neq (0, 0, 0)$ *satisfying the* homogeneous *equation* $Y^2Z = X^3 + aXZ^2 + bZ^3$. *Two projective solutions* $(X, Y, Z), (X', Y', Z')$ *are considered to be equivalent if there exists a scalar* λ *such that* $(X, Y, Z) = (\lambda X', \lambda Y', \lambda Z')$.

Then every point $(x, y) \in E$ corresponds to a projective solution $(x, y, 1)$. We also have the special solution $(0, 1, 0)$ on the *line at infinity.*

Elliptic curves are unique in that they are equipped with an abelian group law. Given two points on the curve, their sum is the reflection across the y-axis of the third point of intersection of the line through them with the curve. Thus the inverse of a point is its reflection across the y-axis, and the identity element of the group is the point at infinity. The only group axiom left to check is associativity; the proof is somewhat involved and the group law on elliptic curves is classical, so we'll omit it here. For a fixed elliptic curve E over $\mathbb{Q}$, the set $E(\mathbb{Q})$ of rational points on this curve is a natural candidate for study. The rational points form a subgroup with respect to the group law on elliptic curves, since the sum of two points on a curve is given, coordinate-wise, by

Date: July 30, 2014.

rational-coefficient rational functions of the coordinates of the two points. The structure of this group is well-understood; indeed,

Theorem 1.3 (Mordell)**.** *The group $E(\mathbb{Q})$ is isomorphic to $T \oplus \mathbb{Z}^r$ where T is a finite subgroup given by the elements of $E(\mathbb{Q})$ with finite order (the so-called torsion subgroup) and r is the rank of the curve.*

1.2. Counting points in $\mathbb{F}_p$

Just as we can study, rational points on elliptic curves, we can try to understand solutions to an elliptic curve that lie in some *finite* field, e.g. $\mathbb{F}_p$. When we work with elliptic curves modulo a prime, it's not enough for the discriminant to be non-zero. We require the discriminant not to vanish modulo p.

Definition 1.4. *For an elliptic curve E we say p is a prime of* good reduction *if the denominators of a and b are coprime to p and the irreducible factors of $f(x)$ in $\mathbb{F}_p[x]$ appear with multiplicity at most 1; equivalently p does not divide the numerator of Δ.*

Consider a fixed a non-singular elliptic curve E with coefficients in $\mathbb{Q}$, and let p be a prime of good reduction. Suppose we wish to count the number of (projective) solutions over $\mathbb{F}_p$ to the modulo-p reduction of this curve. We should expect this number to be roughly $p+1$; there should be approximately p "ordinary" solutions since the variety has dimension 1, and the extra solution comes from the point at infinity. To be precise, we define the error term $a_p = (p+1) - (\#$ of actual solutions), so that the number of solutions over $\mathbb{F}_p$ to this equation is $(p+1) - a_p$. A result of Hasse states

Theorem 1.5 (Hasse)**.** $|a_p| \leq 2\sqrt{p}$.

1.2.1. *The Sato-Tate conjecture for elliptic curves*

In order to understand the distribution of a_p, it's natural to consider the normalized $x_p = a_p/\sqrt{p} \in [-2, 2]$. We can then fix an elliptic curve and ask what the distribution of x_p is as p varies over all primes of good reduction less than N as we send N to infinity. The Sato-Tate conjecture (recently proved for elliptic curves over $\mathbb{Q}$) answers this question for most elliptic curves:

Conjecture 1.6 (Sato-Tate)**.** *Write $x_p = 2\cos\theta_p$. For a generic elliptic curve (one without complex multiplication), θ_p is distributed in $[0, \pi]$ according to $\frac{2}{\pi}\sin^2\theta$.*

Our ultimate goal will be to understand these types of distributions in higher genus, but before we do we need a way to generalize what we mean by a_p; recall that when $g > 1$ there is no group law on the curve itself. In general, it turns out that a_p will be the trace of a particular matrix associated with the modulo p reduction of the curve. Let's see how this looks in genus 1 before moving forward.

1.2.2. *Interpretation in terms of matrices*

One way of looking at the set $E(\mathbb{F}_p)$ of $\mathbb{F}_p$-points of an elliptic curve is as the set of points in $E(\mathbb{F}_p)$ that are fixed by the Frobenius map $x \to x^p$. Thus the set of $\mathbb{F}_p$-points is simply the kernel of the endomorphism $(\mathrm{Frob}_p - \mathrm{Id})$. This is still a difficult problem to tackle directly, but we can simplify matters by restricting to the n-torsion subgroup; that is, the set $E[n] \subset \overline{\mathbb{F}}_p$ consisting of points P such that $nP = O$, where the LHS representing n-fold addition under the curve's group law. It's known that this group is isomorphic to $\mathbb{Z}/n \times \mathbb{Z}/n$ as long as p and n are coprime, and (critically) the Frobenius map commutes with the multiplication map $P \to nP$. Thus it follows

that Frob_p maps $E[n]$ to itself, and this action can be represented by a 2×2 matrix A_p with entries in $\mathbb{Z}/n$ which is invertible when p and n are coprime. We can now apply the identity

$$\det(A_p - I_2) = \det(A_p) - \text{tr}(A_p) + 1.$$

It's known that the modulo-n reduction of the degree (the size of the kernel) of $\text{Frob}_p - \text{Id}$ is equal to the determinant of $A_p - I_2$. Then it's easy to see that since this should hold for all n, the number of solutions over $\mathbb{F}_p$ is $\det(A_p) + 1 - \text{tr}(A_p)$.

According to the Sato-Tate conjecture, the x_p follow a semicircular distribution on $[-2, 2]$. Heuristically, if we think of A_p as a matrix over the complex numbers with trace equal to $p + 1 - \#$ of solutions and determinant p, then $A_p/\sqrt{p}$ is unitary by Hasse. Then the claim that the x_p are distributed according to a semicircular distribution is equivalent to saying that as p varies, $A_p/\sqrt{p}$ is equidistributed in $SU(2)$ according to its Haar measure. Recall that the Haar measure, which exists for any Lie group and is finite as long as the group is compact, is the unique translation-invariant measure with total mass 1; this is explained in greater detail below.

1.2.3. *Complex multiplication and moments*

We aren't completely finished with elliptic curves quite yet. The disclaimer we made earlier was that the Sato-Tate conjecture applied only to elliptic curves without complex multiplication - i.e., curves whose endomorphism ring is simply $\mathbb{Z}$. For curves with CM, the matrix A_p cannot simply be any matrix in $SU(2)$. Since the curve has extra endomorphisms which the Frobenius must commute with, A_p is distributed in some subgroup of $SU(2)$. It turns out there are precisely two possibilities for this subgroup - $U(1)$ and $N(U(1))$, depending on whether one looks in the CM field or not.

Since we may not always have the luxury of an explicit distribution as we do in the generic elliptic curve case, we can work instead with moments. Suppose we didn't know how x_p was distributed precisely; we might find it easier to compute its moments $\mathbb{E}[x_p^n]$ which are in fact enough to determine the distribution uniquely provided some basic analytic conditions hold (which, in this case, they do). Since we know A_p should be equidistributed in $SU(2)$ according to the Haar measure,

$$\mathbb{E}[x_p^n] = \int_{SU(2)} (\text{tr } g)^n \, dg$$

In the case of $SU(2)$, the moment sequence is $1, 0, 1, 0, 2, 0, 5, 0, 14, 0, \ldots$. The odd moments are 0 by symmetry, while the even moments are the familiar Catalan numbers, which (among other things) count the number of walks of a given length in $\mathbb{Z}$ that start and end at the origin while staying to the right of it the entire time. The CM cases also have meaningful combinatorial interpretations; for $U(1)$, the moment sequence is $1, 0, 2, 0, 6, 0, 20, \ldots$, where the $2n$-th moment is $\binom{2n}{n}$. This has a combinatorial interpretation as the number of lattice walks on $\mathbb{Z}$ of length $2n$ that start and end at the origin. In the case of $N(U(1))$, for $n > 0$ the terms are exactly $\binom{2n}{n}/2$, which counts the number of walks of the type just described, up to symmetry with respect to reflection about the origin. This symmetry is somewhat natural; $U(1)$ is a normal subgroup of $N(U(1))$ and $N(U(1))/U(1) \cong C_2$. As a Lie group, this means $N(U(1))$ has $U(1)$ as the connected component of the identity, and component group C_2 (Lie groups are discussed in more detail below).

1.3. **Hyperelliptic curves**

Convinced that there is something of combinatorial intrigue in these moment sequences, we can consider a similar question for a more general class of curves. The natural things to examine next are hyperelliptic curves.

Definition 1.7. *A hyperelliptic curve is an algebraic curve given by an equation of the form* $y^2 = f(x)$ *where* f *is a polynomial of degree at least* 5.

Hyperelliptic curves are typically classified by their genus g, which for equations of the form $y^2 = f(x)$ is simply $\lfloor(\deg f - 1)/2\rfloor$. Thus elliptic curves have genus 1 (in fact, this is part of their precise definition), and hyperelliptic curves have genus at least 2. Let's consider $g = 2$ for now.

Remark 1. What happens when, for instance, f has degree 4? The genus in this case is 1, so we should expect an elliptic curve; yet f is quartic, not cubic. It turns out that by changing coordinates and transforming suitably, any curve of degree 4 can be identified with one of degree 3.

Hyperelliptic curves are not endowed with a natural group law like elliptic curves are, and genus 2 is no exception. The group law for hyperelliptic curves is defined not on the curve itself, but instead on its so-called Jacobian. In general, the Jacobian is an abelian variety associated to any non-singular algebraic curve. In the case of elliptic curves the Jacobian happens to coincide with the curve, which is why the curve itself has a group law. Otherwise, the genus 2 case behaves much the same way as genus 1; the number of (projective) $\mathbb{F}_p$ solutions is $p + 1 - \mathrm{tr}(\mathrm{Frob}_p)$, the trace of Frobenius.

It's natural to expect that, as was the case in genus 1, the matrices $\mathrm{Frob}_p/\sqrt{p}$ should be equidistributed in some compact Lie group. While this has not been proven yet, there is strong empirical evidence suggesting this is the case. Like we saw in genus 1, most curves are "generic" - i.e., have the simplest possible endomorphism ring - and will consequently have $\mathrm{Frob}_p/\sqrt{p}$ equidistributed in some large Lie group. In fact, the set of non-generic curves has measure zero. Those curves that do have a larger endomorphism ring should have $\mathrm{Frob}_p/\sqrt{p}$ distributed in some smaller, Lie subgroup of this large Lie group.

The most general such Lie group in genus 1 was $SU(2)$. In genus 2, and more generally in genus g, this group is $USp(2g)$. Note there is no inconsistency here; $SU(2) = USp(2)$. Thus in genus 2, the matrices Frob_p are usually equidistributed in $USp(4)$. However, as the genus increases the simple dichotomy between generic curves and CM curves disappears. In genus 2, there are 52 exceptional cases, each corresponding to a different Lie subgroup of $USp(4)$. The group theory reveals there are 55 possibilities (subgroups of $USp(4)$), but three of these are either known or strongly conjectured to be unattainable. Still, we will examine these groups as they give rise to a combinatorial problem of the same type.

We expect the distribution of $1/\sqrt{p}$ times the error term in the $\mathbb{F}_p$ point count to be distributed according to the trace of a random matrix chosen according to the Haar measure in some compact Lie group. We can now safely remove ourselves from hyperelliptic curves, and thus from any assumptions about them, and simply consider the distribution of traces in compact Lie subgroups of $USp(4)$. In fact, all but two possible subgroups appear to correspond to some genus 2 curve or other. We'll again use the moments to characterize the distributions, and find that the moment sequences have independent combinatorial interest.

2. Lie groups and trace moments

We've mentioned Lie groups before; we now enter into a brief discussion of their details for the sake of completeness.

Definition 2.1. *A* Lie group *is a manifold with a group structure. We consider only Lie groups which are closed subgroups of* GL_n.

For a set S consider the collection of its subsets T. Formally, $T = \{T : T \subseteq S\}$. We proceed with the definition of a measure.

Definition 2.2. *A* measure *on S is a function $\mu : T \to \mathbb{R}^+ \cup \{0\}$ satisfying $\mu(\emptyset) = 0$ and $\mu(T_1) + \mu(T_2) = \mu(T_1 \cup T_2)$ whenever $T_1 \cap T_2 = \emptyset$. A measure on a Lie group is* translation-invariant *if $\mu(H) = \mu(gH)$ for any subset H of G and $g \in G$.*

Remark 2. In practice, we need to consider the measure only over 'sufficiently nice' subsets of S, but this is an unnecessary discussion for our purposes.

Notice that if μ is a measure, then for any positive real number k, μ_k defined by $\mu_k(T) = k\mu(T)$ for all $T \subseteq S$ is also a measure. In other words, measures can be scaled.

Proposition 2.3. *For a Lie group G there exists a unique translation-invariant measure, up to scaling, called the* Haar *measure of G. When G is compact, we have $\mu(G) < \infty$ (a so-called* finite *measure), so we can normalize the measure to $\mu(G) = 1$.*

2.1. **Representation theory of Lie groups**

For our purposes, a representation of a Lie group G is a homomorphism $\rho : G \to GL(n, \mathbb{C})$ and n is the dimension of the representation. Equivalently, a respresentation is an action of G on $\mathbb{C}^n$. We can also say $V = \mathbb{C}^n$ is a representation of G, so that operations on vector spaces (direct sums, tensor products, wedge powers) are more natural. As usual, a representation is *reducible* if there is a proper subspace $W \subset V$ such that for any $g \in G$ and $w \in W$, $\rho(g)w \in W$. In other words, if W is G-invariant. Otherwise, we call V irreducible.

Definition 2.4. *The* character χ_ρ *of a representation ρ is defined at each point g of G to be $\chi_\rho(g) = tr(\rho(g))$.*

Note that the character is constant on a conjugacy class since trace is preserved under conjugation.

Example 2.5. *The* trivial *representation of G is defined by $\rho_g = I_1$ for all $g \in G$. The* standard *representation of $SU(2)$ is simply a matrix*

$$\begin{pmatrix} x & y \\ -\overline{y} & \overline{x} \end{pmatrix}$$

with $|x|^2 + |y|^2 = 1$ for each element in G. The trace is the sum of the eigenvalues, which are the entries of the diagonal conjugate matrix, namely, $e^{i\theta}$, $e^{-i\theta}$ for some $\theta \in [0, 2\pi]$. Both examples above are irreducible representations.

If V and W are representations of G (call ρ_V and ρ_W the corresponding homomorphisms) $V \oplus W$ is also a representation by letting the action of G on an element $(v, w) \in V \oplus W$ be defined in each subspace (formally, $\rho_{V\oplus W}(g)(v, w) = (\rho_V(g)v, \rho_W(g)w)$). It follows that a direct sum of two representations is reducible and that its character corresponds to pointwise addition of those of the representations involved in the direct sum. Similarly, V and W induce a representation on $V \otimes W$. The representation $\rho_V \otimes \rho_W$ is defined by $(\rho_V \otimes \rho_W)(g)(v \otimes w) = (\rho_V v) \otimes (\rho_W w)$ for $v \in V$, $w \in W$ and extended by linearity to the rest of the space $V \otimes W$. Its trace is $\chi_V \chi_W$.

Most of the properties of the representations of finite groups generalize to compact Lie groups. For instance, we can decompose a representation into irreducible representations, although the pool of possible irreducible representations may be infinite. Similarly, irreducible representations can be distinguished simply by looking at their characters and these form a basis of the space of class functions. Furthermore, integration with respect to the Haar measure allows $\langle \chi_V, \chi_W \rangle = \int_G \chi_V(g)\chi_W(g)d\mu$ to be defined. In addition, it can be proven that the orthogonality relations for finite groups carry over; namely, for irreducible representations χ_V, χ_W we have:

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 0 & V \ncong W \\ 1 & V \cong W \end{cases}$$

where the group has unit measure. In particular, since $\langle\ ,\ \rangle$ is a bilinear form on the characters, $\langle \chi^{\text{triv}}, \chi_\rho \rangle$ counts the multiplicity of χ^{triv} in the decomposition of χ_ρ into irreducible representations.

Definition 2.6. *The* n-th trace moment *of a representation ρ of a Lie group G is the multiplicity of the trivial representation in the n-th tensor power of ρ. By the discussion above it equals:*

$$\langle \chi^{triv}, \chi_{\rho^{\otimes n}} \rangle = \int_G \chi^{triv}(g)\chi_\rho(g)^n d\mu = \int_G \chi_\rho(g)^n d\mu$$

The values for $n = 0, 1, 2, \ldots$ form the trace moment sequence *which clearly consists of nonnegative integers.*

For a Lie group, we'll consider the trace moment sequence of the representation obtained from their standard embedding in $GL(n, \mathbb{C})$, possibly without saying so.

2.2. **Distributions and moment statistics**

By a distribution we refer to a measure μ defined on a set Ω such that $\int_\Omega d\mu(x) = 1$.

Suppose we have a real random variable X distributed according to a measure μ (so $\int_{-\infty}^{\infty} d\mu(x) = 1$). It is a well-known result that in sufficiently well behaved cases (and in particular all the ones we consider), the *moments* or expected values of ^{n}:

$$\mathbb{E}[X^n] = \int_{-\infty}^{\infty} x^n d\mu(x)$$

uniquely determine the distribution, that is, the measure.

Let Y be a random matrix sampled according to the Haar measure in a Lie group G. Let ρ be the representation obtained from the standard embedding of G in $GL(n, \mathbb{C})$, and set $X = \text{tr}(Y)$. Then:

$$\mathbb{E}[X^n] = \int_G \text{tr}(Y)^n d\mu = \langle \chi^{\text{triv}}, \chi_{\rho^{\otimes n}} \rangle$$

so we can determine the distribution of the traces of a random matrix in G (or rather the moments of the traces) by computing the multiplicity of the trivial representation in the decomposition into irreducibles of the n-th tensor power of the standard representation.

Why is this important? The generalized Sato-Tate conjecture [**?**] asserts that to each hyperelliptic curve of genus g we can associate a Lie group $G \subseteq USp(2g)$ (called its Sato-Tate group) in such a way that the distribution of the $x_p = a_p/\sqrt{p}$ in $[-2g, 2g]$ is the same as that of the trace of a random matrix in G. Note that the trace is real since the eigenvalues of a matrix in $USp(2g)$ appear in conjugate pairs. As we've seen, the moments of this trace uniquely determine the underlying distribution, and correspond to the multiplicity of χ^{triv} in the n-th tensor power of the standard representation.

3. Combinatorial interpretations in genus 2 when $G^0 \in \{USp(4), SU(2) \times SU(2), U(1) \times U(1), SU(2) \times U(1)\}$

We've now come to the focus of this paper. We expect that, as they do in genus one, the moment sequences in any genus should have natural combinatorial interpretations in terms of counting lattice walks of a certain kind. Indeed, this is true in the generic case, when the Sato-Tate group is $USp(2g)$; Magyar and Grabiner [MG93] prove in general that the moment sequence in the generic case (namely, the one obtained from matrices sampled at random in $USp(2g)$ according to the Haar measure) in arbitrary genus g counts the number of (integer) lattice walks of length n restricted to the Weyl chamber of g-dimensional space and which start and end at the origin in $\mathbb{Z}^g$.

We'll now attempt to establish equivalence between the moment sequences of some of the 55 exceptional genus 2 cases identified in [**?**] and similar such counting problems. As a way to organize these 55 groups, we use G^0, the connected component of the identity in the group. There are six possibilities for G^0 - $U(1)$, $SU(2)$, $U(1) \times U(1)$, $U(1) \times SU(2)$, $SU(2) \times SU(2)$, and $USp(4)$. We'll consider the various cases in decreasing order of the "size" (not quite dimension) of G^0.

Remark 3. These Sato-Tate groups correspond to the cases in which the normalizer $N(G^0)$ of G^0 has finite index in $USp(4)$. Of course, G is a subgroup of $N(G^0)$ since conjugation by an element of G must permute the connected components and stabilizes the identity element (and thus, its connected component G^0).

3.1. $G^0 = USp(4)$

Of course, we must have $G = G^0 = USp(4)$. Magyar and Grabiner prove that the corresponding moment sequence $1, 0, 1, 0, 2, 0, 5, \ldots$ counts the number of integer lattice walks (i.e. walks with allowed steps $(\pm 1, 0), (0, \pm 1)$) of length n restricted to the first octant (the Weyl chamber, in this particular case) which start and end at the origin. There is a closed form for this sequence; namely, $c_n c_{n+2} - c_{n+1}^2$ where c_k denotes the k-th Catalan number.

3.2. $G^0 = SU(2) \times SU(2)$

Groups in [?]: $SU(2) \times SU(2), N(SU(2) \times SU(2))$

This case accounts for exactly two different Sato-Tate groups - $SU(2) \times SU(2)$ itself, and its normalizer $N(SU(2) \times SU(2))$. The moment sequence of the former is $1, 0, 2, 0, 10, 0, 70, \ldots$ - the $2n$-th term is, in general, the product $c_n c_{n+1}$ of consecutive Catalan numbers. As it happens, this is exactly the number of lattice walks of length n restricted to the first quadrant of the plane. In fact, why the expression $c_n c_{n+1}$ should count the number of walks of this kind is quite difficult, but we can ignore the closed form and explain the equivalence via the algebra.

Proposition 3.1. *The number of lattice walks of length $2n$ confined to the first quadrant which start and end at the origin is given by*

$$\sum_{k=0}^{n} \binom{2n}{2k} c_k c_{n-k}$$

Proof. We count the number of such walks by casework on the number of horizontal steps taken. Supposing there are $2k$ of them (of course, a walk taking an odd number of horizontal steps could not possibly return to the origin), the number of ways to pick k of them to be "right" steps, and the remaining k "left" in such a way that we've never taken more left steps than right is exactly c_k. Analogously, there are c_{n-k} ways to do assign the vertical steps a direction so that the number of walks of this kind is in all

$$\sum_{k=0}^{n} \binom{2n}{2k} c_k c_{n-k}$$

□

This binomial convolution of the Catalan numbers can be interpreted as $\mathbb{E}[(X+Y)^n]$ where X, Y are independent, identically distributed random variables whose even moments are the Catalan numbers (this follows immediately from independence and linearity of expectation). Recall that for a generic elliptic curve, whose Sato-Tate group is $SU(2)$, the even moments are precisely the Catalan numbers. Since $SU(2) \times SU(2)$ embeds diagonally in $USp(4)$, and has as its Haar measure

the square of the Haar measure on $SU(2)$, the trace of a random matrix in $SU(2) \times SU(2)$ is distributed as $X+Y$. Thus $\mathbb{E}[(X+Y)^n]$, which counts the number of first quadrant walks starting and ending at the origin, is the trace moment sequence for the Sato-Tate group $SU(2) \times SU(2)$.

The other possible Sato-Tate group, $N(SU(2)\times SU(2))$, has moment sequence $1, 0, 1, 0, 5, 0, 35, \ldots$; for $n > 0$, the $2n$-th term is $c_n c_{n+1}/2$. Again, we won't prove that this closed form is valid for the moment sequence; rather, we'll show the moment sequence and the counting problem agree, circumventing the closed form altogether. The closed form is really only for completeness and notational convenience.

Proposition 3.2. *The number of essentially different first-quadrant lattice walks of a given positive length that start and end at the origin, where two paths are considered equivalent if they are reflections of one another about the line $y = x$, is given by*

$$\frac{1}{2}\sum_{k=0}^{n} \binom{2n}{2k} c_k c_{n-k}, n > 0$$

Proof. Since no path can be its own reflection when $n > 0$, there are precisely

$$\frac{1}{2}\sum_{k=0}^{n} \binom{2n}{2k} c_k c_{n-k}$$

inequivalent paths.

□

The algebraic motivation is as follows : $N(SU(2) \times SU(2))$ is generated by $SU(2) \times SU(2)$ together with the single, order two matrix

$$\begin{bmatrix} 0 & -I_2 \\ -I_2 & 0 \end{bmatrix}.$$

Thus exactly half the matrices in $N(SU(2) \times SU(2)$ have trace zero, while the rest have trace distributed according to the distribution on $SU(2) \times SU(2)$.

3.3. $G^0 = U(1) \times SU(2)$

Groups in [?]: $U(1) \times SU(2), N(U(1) \times SU(2))$

Again, there are only two Sato-Tate groups of this kind - $U(1) \times SU(2)$ itself, and its normalizer $N(U(1) \times SU(2))$ which contains $U(1) \times SU(2)$ as an index 2 subgroup. The moment sequence for $U(1) \times SU(2)$ is $1, 0, 3, 0, 20, 0, 175, \ldots$ - the $2n$-th term is $c_n b_{n+1}/2$ in general. Based on what the moment sequences for $U(1)$ and $SU(2)$ counted in genus one, we might expect

Proposition 3.3. *The number of upper half-plane lattice walks that start and end at the origin is*

$$\sum_{k=0}^{n} \binom{2n}{2k} c_k b_{n-k}$$

Proof. If we make $2k$ vertical steps, there are c_k ways to arrange them so that the path never falls below the x-axis, and b_{n-k} ways to pick the horizontal steps. Summing over k, the total number of such walks is

$$\sum_{k=0}^{n} \binom{2n}{2k} c_k b_{n-k}$$

□

Note that, once again, we haven't shown that the sum in question is equal to the closed form provided. We're only interested in establishing equivalence between the moment sequences and counting problems, not so much in the problems themselves.

This binomial convolution can be interpreted as $\mathbb{E}[(Z+W)^n]$ for independent random variables Z, W where Z has the Catalan numbers as its even moments, and W has the central binomial coefficients. In the genus one case, we saw the moment sequence for $SU(2)$ was exactly the Catalan numbers, and the moment sequence for $U(1)$ was the central binomial coefficients. What's more, $U(1) \times SU(2)$ embeds diagonally in $USp(4)$ and has as its Haar measure the product of the Haar measures on $U(1)$ and $SU(2)$, so that the trace of a random matrix in $U(1) \times SU(2)$ is distributed as $Z + W$. Thus the moment sequence is simply $\mathbb{E}[(Z+W)^n]$, which is the binomial convolution we obtained by counting.

As was the case before, there is only one other group with this connected component, $N(U(1) \times SU(2))$. This group has moment sequence $1, 0, 2, 0, 11, 0, 90, \ldots$. For $n > 0$, the $2n$-th term is $(c_n b_{n+1} + c_n)/2$.

Proposition 3.4. *The moment sequence for $N(U(1) \times SU(2))$ counts the number of essentially different upper half-plane lattice walks that start and end at the origin, where two paths are considered equivalent if they are reflections of one another about the y-axis*

Proof. When $n = 0$ there is one such path (the empty path), and for $n > 0$ only the paths that lie entirely along the y-axis (of which there are c_n) can be their own reflections, so principle of inclusion-exclusion with Proposition 3.3 means there are $(c_n b_{n+1} + c_n)/2$ such paths in all. □

3.4. $G^0 = U(1) \times U(1)$

Groups in [?]: $F, F_a, F_c, F_{ab}, F_{ac}, F_{a,b}, F_{ab,c}, F_{a,b,c}$

The next class of groups have $G^0 = U(1) \times U(1)$ - there are eight of these groups, which can be further classified (although not completely) by their component group G/G^0.

Component group $G/G^0 = C_1$

Here the component group is trivial, so $G = G^0 = U(1) \times U(1)$. This group is denoted by F in [?], a convention which we too will use. The moment sequence in this case is $1, 0, 4, 0, 36, 0, 400, \ldots$, where in general the $2n$-th term is b_n^2. It's not hard to see that this is the number of lattice walks of length n in the plane that start and end at the origin.

Indeed, the number of such walks is exactly the same as the number of walks on length n on a diagonal lattice (whose basis vectors with respect to the standard basis are $(1,1)$ and $(-1,1)$) which start and end at the origin, since we can go from walks of one type to the other by rotating by $\pi/4$. To count the number of diagonal lattice walks, remark that exactly n of the $2n$ steps must be steps in the positive x-direction, and n of the $2n$ steps must be steps in the positive y-direction. These choices uniquely determine the identity of each step and the resulting path must return to the origin, so in all there are $\binom{2n}{n}^2$ paths of this kind.

Component group $G/G^0 = C_2$

There are 3 different groups with connected component $U(1) \times U(1)$ and component group C_2; in [**?**] they are denoted by F_a, F_c, and $F_{a,b}$. In the first case, the moment sequence is $1, 0, 3, 0, 21, 0, 210, \dots$ where the $2n$-th term is $\frac{1}{2}(b_n^2 + b_n)$. This counts the number of distinct lattice walks starting at and returning to the origin up to reflection about, say, the y-axis. Indeed, each of the b_n^2 walks has a reflection different from itself except for the b_n that are confined to the y-axis; the formula follows.

The moment sequence for the group F_c is $1, 0, 2, 0, 18, 0, 200, \dots$ where the $2n$-th term is $\frac{1}{2}b_n^2$. This counts the number of distinct lattice walks of length n starting and ending at the origin, up to reflection about the line $y = x$; indeed, every path has a reflection different from itself.

Finally, the group F_{ab} has the same moment sequence - $1, 0, 2, 0, 18, 0, 200, \dots$. Again, he $2n$-th term in general is $\frac{1}{2}b_n^2$. This counts the number of distinct lattice walks of length n starting and ending at the origin, up to a rotation of $\pi/2$ about the origin. It's not hard to see that once more, every path has a rotation different from itself. What may not be so clear, however, is why we chose these particular order two symmetries for these groups. This will become apparent shortly; we'll see that roughly, a represents reflection about the y-axis, b represents reflection about the x-axis, and c represents reflection about the line $y = x$. This explains, for instance, why there is no group F_b; it is the same as the group F_a.

Component group $G/G^0 = C_4$

The group F_{ac}, as we should expect given the cases we've seen so far, has moment sequence which counts the number of lattice walks of length n that start and end at the origin, and which are inequivalent up to the transformation ac. Given that a represents reflection about the vertical axis, and c represents reflection about the line $y = x$, the transformation ac represents counterclockwise rotation by $\pi/4$. Clearly for $n > 0$ no path is its own rotation, and so the moment sequence $1, 0, 1, 0, 9, 0, 100, \dots$ with $2n$-th term $\frac{1}{4}\binom{2n}{n}^2$ agrees with what we should expect.

Component group $G/G^0 = D_2$

The same is true for the two groups with component group D_2 - $F_{a,b}$ and $F_{ab,c}$. Indeed, the moment sequence of $F_{a,b}$ is $1, 0, 2, 0, 12, 0, 110, \dots$ with $2n$-th term $(b_n^2 + 2b_n)/4$. We'd expect this to count the number of lattice walks of length $2n$ that start and end at the origin, equivalent up to reflection about the horizontal and vertical axes. This is exactly what happens - the only walks that are equal to reflections of themselves about either axis (note ab corresponds to a $\pi/2$ rotation about the origin, which fixes no path) are those that lie entirely on a single axis. For $n > 0$ there are $2b_n$ of these and the claim follows.

The group $F_{ab,c}$ is slightly more straightforward. The symmetries in question here are a $\pi/2$ rotation about the origin, and reflection about the lines $y = x$ and $y = -x$. Each of these symmetries fixes no paths with $n > 0$, so the $2n$-th term of the moment sequence should be $\frac{1}{4}b_n^2$ for $n > 0$; it should come as no surprise that it is.

Component group $G/G^0 = D_4$

This group $F_{a,b,c}$ has the largest possible component group of a Sato-Tate group with connected component $U(1) \times U(1)$. In this case the moment sequence is $1, 0, 1, 0, 6, 0, 55, \ldots$ with $2n$-th term equal to $\frac{1}{8}(b_n^2 + 2b_n)$ in general. We claim that for $n > 0$ this counts the number of lattice walks of length $2n$ that start and end at the origin, up to equivalence with respect to all symmetries of the square.

Indeed, it's not hard to see that the only paths that are sent to themselves under any of these symmetries are those that lie entirely on one axis. Once more there are $2b_n$ of these paths and no others, and these paths are fixed only by reflection about the axis on which they lie, so there should be $\frac{1}{8}(b_n^2 + 2b_n)$ inequivalent paths, as desired.

4. Combinatorial interpretations in genus 2 when $G^0 \in \{SU(2), U(1)\}$

The cases we've seen so far have been fairly simple; in each, the moment sequences have been very clearly related to lattice walks of some sort. The prescence of two groups in the decomposition of G^0, e.g. $U(1) \times SU(2)$, led to simultaneous restrictions on each of the two coordinates of the walk. Finally, the component group G/G^0 was always a subgroup of D_4, so that its action on the paths was natural.

When we move to the two "smaller" cases of $U(1)$ and $SU(2)$ we see a somewhat different behavior. There is now only one group as opposed to two, and there are many more possibilities for the component group. In general, the connected component places a restriction on the path in only one of the coordinate directions; restrictions and/or symmetries in the other direction depend on the component group.

We'll now explain a couple of methods by which we can relate component groups to counting problems.

The first keeps within the basic paradigm of planar lattice walks that we've been working with, in which the component groups act by imposing restrictions or symmetries on the unconstrained axis of walk. The counting problems from this perspective fit more naturally with the counting problems for the larger component groups, as they count walks in two dimensions.

The second method involves interpreting the moment sequences as counting closed walks on the number line together with some auxiliary graph, where a move entails making a move on the graph and a move on the number line and the walks on each must return to their starting point. The connected component restrictions are inherited from genus 1, and the component group acts by restriction or symmetry on the graph walk. In this method the component groups act slightly more naturally.

In general, the component groups in these cases are subgroups either of $S_4 \times C_2$ or $D_6 \times C_2$, the two possible maximal subgroups. The interpretation for $S_4 \times C_2$ (the corresponding group is $J(O)$), and, by extension, several of its subgroups, works most naturally in the setting of the second method. In the case of $D_6 \times C_2$ and its subgroups, the second "method" is really just a different way of thinking of the first, and the first is more natural.

4.1. $G^0 = SU(2)$

Groups in [?]: $E_1, E_2, E_3, E_4, E_6, J(E_1), J(E_2), J(E_3), J(E_4), J(E_6)$

For the $SU(2)$ cases, the models mentioned above are not exceptionally different in substance, as $S_4 \times C_2$ does not come up. We'll nonetheless explain them both in order to lay out the basic model the remaining groups are to follow.

The first idea is to let the component group act on and restrict in the plane. In this case, however, it will prove to be better to look at *diagonal* lattice walks, in which each step taken is of the form $(\pm 1, \pm 1)$. Recall that in genus 1, $SU(2)$ imposed the restriction that the path should stay to one side of the number line and return to the origin. Since we have two coordinate directions to work with now, it makes sense for this restriction to be placed on one of them, say the horizontal. The vertical movement is controlled by the component group.

When $G^0 = SU(2)$, all component groups are cyclic or dihedral. In the cyclic cases, C_k, the component group restricts the vertical motion by requiring that the path ends at a y-coordinate divisible by $2k$. In the dihedral cases, D_k, the component group does the same thing, but also identifies a path with its reflection in the x-axis.

Since we make diagonal lattice walks, each move requires choice of a horizontal and vertical direction; conversely, such a choice determines the step uniquely. Since these two directions are independent, we can count them separately and multiply. In each case there are c_n ways to take steps along the horizontal axis. Depending on the value of k, and whether the component group is C_k or D_k, we will get various different numbers of walks that end at a y-coordinate divisible by $2k$. The proofs that these formulas, taken from [**?**] are correct is not difficult, but it's simpler to refer to the relevant entries in [**?**]

We now mention how to think about these cases in terms of the second method. Recall that the group $SU(2)$ "lived" in one dimension in genus 1, so it might be better to think of the $SU(2)$ case within the number line paradigm instead of in terms of planar walks. To account for the extra term in the moment sequences, we must simultaneously look at a walk on an auxiliary graph which depends on the component group. In the cyclic and dihedral cases, this graph is a $2k$-cycle; it's clear that for these cases this is identical, in essence, to the first model. On the other hand, we aren't forced to pass to diagonal lattice walks and $SU(2)$ restricts as it did in genus 1.

4.2. $G^0 = U(1)$

Groups in [?]: $C_1, C_2, C_3, C_4, C_6, D_2, D_3, D_4, D_6, T, O, J(C_1), J(C_2), J(C_3)$, $J(C_4), J(C_6), J(D_2), J(D_3), J(D_4), J(D_6), J(T), J(O), C_{2,1}, C_{4,1}, C_{6,1}, D_{2,1}, D_{4,1}, D_{6,1}$, $D_{3,2}, D_{4,2}, D_{6,2}, O_1$.

As shown in [**?**], these subgroups occur as finite subgroups of $SO(3) \times C_2$ $(N(U(1))/U(1))$ satisfying certain rationality conditions. Recall they are all subgroups of $S_4 \times C_2$ or $D_6 \times C_2$; thus ideally any kind of combinatorial interpretation for the moment sequences of these groups would respect the Hasse diagram (of the lattice of subgroups) of the Lie groups to which they correspond, namely $J(O)$ and $J(D_6)$. These Hasse diagrams are closely related to the lattice of subgroups of these two maximal groups in $USp(4)$ (but not completely, since subgroups might be conjugate in $USp(4)$ but not in $J(O)$ or $J(D_6)$). Their descriptions are included in the Appendix.

Again, it will be possible to look in the plane or at the number line together with an auxiliary graph. We've made this distinction clear before and the component groups for $U(1)$ are much more complicated than those for $SU(2)$, so instead of classifying by method we'll classify by maximal subgroup.

4.2.1. *G/G^0 a subgroup of $S_4 \times C_2$*

First Method

The first way to try and make sense of this group will be to assign it an action on (diagonal) lattice walks in the plane. As before, we should expect the $U(1)$ component to restrict one of the coordinate directions, and the component group the other. Unfortunately, there is no natural "modularity condition" associated with S_4, so we'll work with an action of the group instead. Note that S_4 acts in the usual way on *pairs* of choices of vertical move. Indeed, for any two consecutive steps we must choose a vertical movement direction for each, which can be done in $2^2 = 4$ ways, and S_4 acts on these four possibilities. We can assign the C_2 component of $S_4 \times C_2$ an action on the horizontal steps which identifies a sequence of horizontal moves with its reflection in the y-axis. Then the moment sequence for $J(O)$, whence comes $S_4 \times C_2$, counts the number of paths that return to the origin in the x-direction, up to the S_4-action on the y-coordinate choices and the reflection from C_2. Again, horizontal and vertical choices are taken independently, so we can just multiply the corresponding sequences. The sequence for $U(1)$ is of course just b_n; the proof that the other term in the moment sequence from [**?**] the number of paths of length $2n$ along a single direction up to this S_4 action is tricky, so we'll simply refer to the [**?**].

Many of the other component groups are subgroups of $S_4 \times C_2$. In many cases, the interpretation carries over quite naturally; in particular, the groups A_4, D_4, C_3, C_2, C_1 can embed in S_4 in such a way that their moment sequences count the number of inequivalent walks up to the action of the corresponding subgroup of S_4 on the pairs of vertical move choices. There is some art to picking the embedding - for instance, C_2 must embed as the group generated by a double transposition; no ordinary transposition will do. Unfortunately, the subgroups C_4 and D_3 of S_4 do not follow this paradigm, so we have to look at them the way we looked at cyclic and dihedral groups before; namely, as imposing restrictions on the vertical move choices in the walk. In this section, we explain how the classification of the subgroups is deduced. Then, in the following one, we explain an alternate equivalent counting problem (based on symmetries on a K_4) and we give a proof of our claim about the model working when restricted to a certain subgroup.

Classification of the component groups of the subgroups of $J(O)$

Things are slightly more complicated when the component group is a subgroup of $S_4 \times C_2$ with non-trivial projection onto the C_2 component. When the component group is of the form $J(C_k)$ or $J(D_k)$ (i.e. we have a direct product) it is simply a matter of identifying paths with their reflections, with the restriction inherited from the group C_k or D_k. In the exceptional cases C_4 and D_3, the behavior is the same (i.e. direct product with C_2 identifies walks on the number line with their reflections), but again is best explained by the other model.

Sometimes, however, the subgroups are more interesting; they can be onto each component in the product, but not onto overall. This essentially amounts to finding non-trivial homomorphisms from the subgroups of S_4 to C_2.

From S_4, there is only the sign homomorphism; indeed, A_4 is the only normal subgroup of index 2 in S_4, and is killed by the sign homomorphism. Since A_4 has only the Klein four-group as a normal subgroup, with index 3, A_4 has no non-trivial homomorphisms to C_2.

All other subgroups of S_4 are either cyclic or dihedral. The groups D_2, D_4 do in fact have nontrivial homomorphisms onto C_2. If we let x, y be the generators, so that $x^k = xyxy = y^2 = 1$, then a nontrivial homomorphism is uniquely specified by the images of x and y; the condition that this homomorphism be nontrivial requires that x and y are not both sent to 1. Thus there are 3 possible nontrivial homomorphisms onto C_2. In the case of D_2, these are interchanged by an outer automorphism and all isomorphic to the sign homomophism. For D_4, there are two distinct nontrivial homomorphisms up to up to outer automorphism, one of which is isomorphic to the sign homomorphism. These correspond to the groups $D_{4,1}, D_{4,2}$.

All that remain are the cyclic groups. None of these have index 2 in S_4 or A_4, and so they are normal subgroups only of the dihedral groups. When they occur as subgroups of a dihedral group, (notice there is a unique embedding of C_k in D_k up to conjugation) they can or not inherit a sign assignment depending on what this was on the dihedral supergroup. It is this way that $C_{2,1}$ and $C_{4,1}$ arise and the specifics of which of the $D_{i,j}$ they come from are shown in the Appendix.

Second Method

Unlike in the $SU(2)$ case, the second interpretation involving a number line walk coupled with a walk on an auxiliary graph is more subtle and genuinely different from planar action. We will use an auxiliary K_4, the complete pseudograph (i.e. with loops) on four vertices. We explain this interpretation now. We begin with a remark that will shorten the work to be done.

Remark 4. The groups whose notation includes a J (corresponding to the adjoining of the matrix called J in [**?**]) correspond to a component group that inherits from the C_2 in $SO(3) \times C_2$. In every case, this is interpreted as identifying symmetric across the origin walks in the number line part of the counting problem. Except for $J(O)$ and $J(D_6)$, which we include for being the maximal groups, we thus limit our mention of these groups, as it suffices to describe the group to which J was adjoined.

We consider, as an auxiliary graph, a K_4 (cocmplete graph in 4 vertices) with loops at each of its vertices. The basic idea is to let S_4 (or a subgroup of it) act on this K_4 and determine which symmetries to ignore while a presence of the C_2 identifies paths in the number line that are reflections over the origin of each other. A more detailed description follows, starting by $J(O)$.

Proposition 4.1. *The $2n$-th trace moment for $J(O)$ counts the number of closed walks of length n in a K_4 with loops at each vertex where two walks are considered equivalent if one can be obtained from the other by applying an S_4 symmetry to the vertices of K_4, coupled with an independent origin-returning walk of length $2n$ on the number line up to reflection across the origin.*

Proof. As usual, the origin returning walks on the number line up to reflection introduce a factor of $\frac{1}{2}b_n$, so we restrict our attention to the S_4 portion.

In order to count the number of non-isomorphic walks in the K_4, label the vertices in the graph as a, b, c, d. Then a closed walk of length n corresponds to a word of length n with the characters a, b, c, d: the i-th letter corresponds to the vertex which the walk is at after taking i steps. Since we are ignoring S_4 symmetries, we could without lost of generality choose the initial vertex such that it coincides with the final one, thus making the walk closed. So, for instance, the word "*bcd*" corresponds to the closed walk $d \to b \to c \to d$ of length 3 and it is equivalent to other 23 walks which are in its S_4 orbit.

Hence, the problem is equivalent to counting the number of words of length n on a 4-letter vocabulary where 2 words are considered equivalent if related by a S_4 symmetry on the letters. This is equivalent to partitioning the set $\{1, 2, \ldots, n\}$ into at most 4 parts (each corresponds to a letter and the S_4 symmetries come from not distinguishing between the part) . [**?**] sequence A124303 counts exactly this quantity, and its closed form is the same as the one for $J(O)$ in [**?**]. □

We could expect that this same counting problem would work for any subgroup of $J(O)$ by restricting to the appropriate component group for the symmetries. Recall the subgroups of S_4 are $A_4, D_4, D_3, D_2, C_4, C_3, C_2, C_1$. This is almost true, except for two aspects:

(1) Care must be taken with groups of the form $C_{i,j}, D_{i,j}$ as the j represents a particular homomorphism from the component group onto C_2.
(2) The model does not hold for the cases related to D_3 and C_4 ($J(D_3), D_3, D_{3,2}, J(C_4), C_4, C_{4,1}$). We provide provisionary explanations for these.

Indeed, except for these cases, this 'restriction of symmetries' model respects the Hasse diagram of $J(O)$. We first deal with the T, D_k, C_k cases (we remarked above how the presence of a J affect these), then explain the $C_{i,j}, D_{i,j}$ ones and finally provide the provisionary explanations for those related to D_3, C_4.

Proposition 4.2. *Restricting the counting problem from $J(O)$ to the appropriate group of symmetries provides a counting problem for $T, D_4, D_2, C_4, C_2, C_1$.*

Proof. For all cases, the zeroth moment is 1 so we won't consider it (although if appropriately interpreted what follows applies).

We begin with T, the component group A_4. Recall A_4 consists of the set of 3-cycles (8 of these), double transpositions (3 of these) and the identity. Recall the interpretation of this problem in terms of counting words. As we are counting the number of orbits on length n words under the action of A_4, by Burnside's lemma it suffices to count how many words are fixed by each element of A_4. Clearly, the identity fixes all 4^n words. Each 3-cycle fixes precisely one word, that which consists entirely of the letter not permuted by the $3-cycle$. The double transpositions do not fix any words. Thus, Burnside's lemma gives the counting formula $\frac{1}{12}(2^{2n}+8)$ for $n \geq 1$ and the claim follows.

For D_4, the generators are a 4-cycle, e.g. $(abcd)$, and a non-adjacent transposition such as (ac). In this case, every word has orbit of size 8 except those which consist of only two non-adjacent letters. There are 2^n of these, each with an orbit of size 4. Thus, we have $\frac{1}{8}(2^{2n}+2\cdot 2^n)$ for $n \geq 1$.

For D_2, we need to be careful with the choice of generators. We use the D_2 consisting of the identity and the double transpositions. Then, every word has an orbit of size 4 and the formula $\frac{1}{4}(2^{2n})$ follows.

For C_2, every word has orbit of size 2 and we obtain $(\frac{1}{2})2^{2n}$.

C_1 acts trivially, so there are 2^{2n} inequivalent words in this case.

□

This takes care of proving that this model holds for the basic cases we claimed. We now talk about the first bullet point above, namely, how to extend this interpretation to the $D_{i,j}, C_{i,j}$ cases.

Extension of the combinatorial problems to O_1 and $D_{i,j}, C_{i,j}$

Recall the work made classifying the subgroups of $J(O)$. In particular, remember the j in $D_{i,j}$ specifies a certain sign assignment to the elements of D_i. The key idea is:

Proposition 4.3. *The kernel of the homomorphism onto C_2 (sign assignment) defines what symmetries to consider on the auxiliary graph K_4. The presence of such homomorphism identifies symmetric walks with respect to the origin in the number line. This gives a counting problem for $O_1, D_{4,2}, D_{4,1}, D_{2,1}, C_{2,1}$.*

Proof. For the homomorphisms corresponding to $O_1, D_{4,2}, D_{4,1}, D_{2,1}, C_{2,1}$, the kernels are A_4, C_4, D_2, C_2, C_1, respectively. We can see that, indeed, their formulae in Table 10 of [**?**] are those for T, C_4, D_2, C_2, C_1 (the connected components of Sato-Tate groups such that these connected components are isomorphic to the mentioned kernels) multiplied by a factor of $\frac{1}{2}$. The halving comes from identifying symmetric walks in the number line. □

The cases D_3 and C_4

We mentioned above that the cases D_3 and C_4 are not well explained by the symmetry group they induce as a subgroup of S_4. Instead, we profit more by interpreting them using the auxiliary graph picture that applies to cyclic and dihedral groups as the model for $J(D_6)$ presented below. Thus D_3 acts on a 6-cycle, and C_4 on an 8-cycle, each taken together with the usual walk on the number line. All the problematic cases mentioned in bullet point (2) above can be resolved by a mixture of this interpretation and the idea of choosing an appropriate cycle according to the kernel. More precisely

Proposition 4.4. *The kernel of the homomorphism onto C_2 (sign assignment) defines what cyclic graph to consider and which symmetries to ignore. The presence of such homomorphism identifies symmetric walks with respect to the origin in the number line. This gives a counting problem for $D_3, C_4, D_{3,2}, C_{4,1}$.*

Proof. For the homomorphisms corresponding to $D_3, C_4, D_{3,2}, C_{4,1}$, the kernels are D_3, C_4, C_6 C_2, respectively. The corresponding problems count closed walks in a 6-cycle, 8-cycle, 12-cycle, 4-cycle, respectively (and the formulae for these can be found on the OEIS), and up to D_3, C_4, C_6, C_2 symmetries (which mean fixing a vertex in the cyclic cases and identifying reflections across this vertex in the dihedral one). In the last two cases, the presence of a non-trivial homomorphism onto C_2 identifies walks in the number line in the usual manner, thus halving the result. □

4.2.2. *Subgroups of $J(D_6)$*

Groups in [?]: $J(D_6), J(D_3), D_{6,2}, D_{6,1}, J(C_6), D_6, C_6, C_{6,1}D_3, D_{3,2}, J(C_3), D_2, D_{2,1}, J(C_2), J(C_1)$, C_1

Remark 5. As mentioned under "The cases D_3 and C_4" the method described here provides a combinatorial problem for all the Sato-Tate groups of the forms $J(C_k), J(D_k), C_{i,j}, D_{i,j}, C_k, D_k$ (that is, all the $U(1)$ cases except T, O, O_1, $J(T)$, $J(O)$).

Remark 6. As mentioned before, in this case, the first method and second method are just two different ways of interpreting the same counting problem, so we'll just describe the method which uses the auxiliary graph.

We'll need the following lemma:

Lemma 4.5. *Let ζ be a primitive $2k$-th root of unity. Then the number of closed walks of length n starting at a fixed vertex in a $2k-$cycle is*

$$\frac{1}{2k}\sum_{j=0}^{2k-1}(\zeta^j+\zeta^{-j})^n$$

Proof. Letting x represent a step clockwise and x^{-1} a step counterclockwise, a standard generating function argument reveals we're interested in the sum

$$\sum_t [x^{2kt}](x+x^{-1})^n$$

where t varies over $\mathbb{Z}$. We can now apply the usual roots of unity filter, so that the sum in question is $1/(2k)$ times the sum we get by substituting for x the powers $\zeta^j, 0\leq j\leq 2k-1$, and the result follows. □

Notice that as described in section 5.1.1 of [**?**], the way of computing the distributions (and therefore the trace moment sequences) involves averaging various powers of sums of roots of unity (called $r(h)$ in [**?**]) in the same way as the lemma above does.

Proposition 4.6. *We find a combinatorial interpretation for the trace moment sequences of all subgroups of $J(D_6)$ as follows:*

1. *As in all the $U(1)$ cases, we count the closed walks of length $2n$ in the number line.*
2. *If the group is of the form $J(C_k), J(D_k), C_{i,j}, D_{i,j}$, meaning the inherited homomorphism onto C_2 (sign assignment) from $SO(3)\times C_2$ is non-trivial, we identify reflections across the origin on this walk on the number line. Else, we don't.*
3. *The kernel of this homomorphism is C_k or D_k. In either case, we consider closed walks of length $2n$ in a $2k$-cycle. We ignore C_k or D_k symmetries, respectively.*

Proof. We limit ourselves to describe what each of the bullet points counts:

(1) This corresponds to the central binomial coefficients, b_n.
(2) When we identify reflected walks, we are multiplying by a factor of $\frac{1}{2}$.

C_k fixes a vertex and counts closed walks starting there. D_k additionally identifies walks that are reflections of each other across this vertex. The number of closed walks of length $2n$ in a $2k$-cycle can be computed according to the lemma below and equals the required values from [**?**] because of the explanation that follows this lemma. □

5. Further directions

5.1. **Role of Lie groups in combinatorial interpretations**

Although most combinatorial itnerpretations have been determined and we know that for the connected groups it consists on counting origin-returning walks in the Weyl chamber of the group, it is of interest to systematically understand how the component group comes into play. For most basic cases in genus 1 this occurs by the component group imposing a series of symmetries to be ignored. However, since more complicated groups (e.g. $S_4\times C_2$ which is the component group for a Sato-Tate group with connectedcomponent of the identity $U(1)$) do not act naturally in the plane, the current combinatorial interpretations become somewhat more *ad hoc*. The objective is to develop a theory that applies to all 55 Sato-Tate groups and could possibly generalize to provide the moment sequences of Sato-Tate groups of curves of higher genus.

5.2. **Looking at a_2**

In genus 2 the characteristic polynomial of the Frobenius map is of the form $L_p(t) = t^4 + a_1t^3 + a_2t^2 + a_1t + 1$. Formulae for the moment sequences of the distribution of the a_2 in genus 2 are known, but their combinatorial interpretations are not well understood. It can be expected that there exist some as these sequences correspond to multiplicities of the trivial representation in the tensor powers of the second-wedge power of the standard representation.

5.3. **Looking at genus 3**

There exist 15 possible identity components. However, neither is there full data about the possible component groups available nor is it practical to analyze it, as the partial progress has found hundreds of them. Some beginning steps would consist of finding interpretations for the sequences obtained from the connected cases and possibly some of their most simple variations.

Indeed, the cases in which the normalizer of G^0 has finite index in $USp(6)$ seem to behave similarly by letting each restriction or symmetry take place in one of the coordinates.

6. Acknowledgements

The authors would like to thank the SPUR program at MIT for allowing them the opportunity to do this research. In particular, they appreciate the help of SPUR coordinators Prof. Pavel Etingof and Prof. David Jerison in discussing and providing direction for their project. They also thank their mentor David Corwin for guiding the research, teaching them some new mathematics, and generally improving the quality of writing in the paper. In addition, they would like to extend their gratitude Prof. Drew Sutherland for suggesting the project and discussing it with them. Finally, they thank Dr. Slava Gerovitch for organizing the SPUR program.

7. Appendix

7.1. **Hasse diagram for** $J(O)$

(1) $J(D_3), J(T), O_1, O, J(D_4)$ are the maximal subgroups of $J(O)$
(2) $J(C_3), T, J(D_2)$ are the maximal subgroups of $J(T)$
(3) $T, D_{3,2}, D_{4,1}$ are the maximal subgroups of O_1
(4) T, D_3, D_4 are the maximal subgroups of O
(5) $D_4, D_{4,1}, J(C_4), D_{4,2}, J(D_2)$ are the maximal subgroups of $J(D_4)$
(6) $J(C_3), D_3, D_{3,2}, J(C_2)$ are the maximal subgroups of $J(D_3)$
(7) D_2, C_4 are the maximal subgroups of D_4
(8) $D_2, D_{2,1}, C_{4,1}$ are the maximal subgroups of $D_{4,1}$
(9) $J(C_2), C_4, C_{4,1}$ are the maximal subgroups of $D_{4,1}$
(10) $D_{2,1}, C_4$ are the maximal subgroups of $D_{4,2}$
(11) $D_2, D_{2,1}, J(C_2)$ are the maximal subgroups of $J(D_2)$
(12) $C_3, J(C_1)$ are the maximal subgroups of $J(C_3)$
(13) C_3, C_2 are the maximal subgroups of D_3
(14) $C_3, C_{2,1}$ are the maximal subgroups of $D_{3,2}$
(15) C_2 is the maximal subgroup of D_2
(16) C_2 and $C_{2,1}$ are the maximal subgroups of $D_{2,1}$
(17) $C_2, J(C_1), C_{2,1}$ are the maximal subgroups of $J(C_2)$
(18) C_2 is the maximal subgroup of C_4 and $C_{4,1}$
(19) C_1 is the maximal subgroup of $C_3, C_2, J(C_1)$ and $C_{2,1}$

7.2. **Hasse diagram for** $J(D_6)$

(1) $J(D_3), J(C_6), D_6, D_{6,1}, D_{6,2}$ are the maximal subgroups of $J(D_6)$
(2) D_3, C_6, D_2 are the maximal subgroups of D_6
(3) $D_{3,2}, D_3, C_{6,1}, D_{2,1}$ are the maximal subgroups of $D_{6,1}$
(4) $D_{3,2}, C_6, D_{2,1}$ are the maximal subgroups of $D_{6,2}$
(5) $J(C_3), J(C_2), C_{6,1}, C_6$ are the maximal subgroups of $J(C_6)$
(6) $D_3, D_{3,2}, J(C_3), J(C_2)$ are the maximal subgroups of $J(D_3)$
(7) C_3, C_2 are the maximal subgroups of D_3
(8) C_3, C_2 are the maximal subgroups of C_6
(9) $C_3, C_{2,1}$ are the maximal subgroups of $C_{6,1}$
(10) $C_3, C_{2,1}$ are the maximal subgroups of $D_{3,2}$
(11) $C_3, J(C_1)$ are the maximal subgroups of $J(C_3)$
(12) C_2 is the maximal subgroup of D_2
(13) $C_2, C_{2,1}$ are the maximal subgroups of $D_{2,1}$
(14) $C_2, C_{2,1}, J(C_1)$ are the maximal subgroups of $J(C_2)$
(15) C_1 is the maximal subgroup of $D_2, D_{2,1},$ and $J(C_1)$

References

[1] K. Kedlaya, A. Sutherland. Hyerelliptic Curves, L-polynomials, and Random Matrices. `http://arxiv.org/pdf/0803.4462.pdf`, 2009.
[2] F. Fite, K. Kedlaya, V. Rotger, A. Sutherland. Sato-Tate distributions and Galois endomorphism modules in genus 2. `http://arxiv.org/pdf/1110.6638v2.pdf`, 2011.
[3] *The On-Line Encyclopedia of Integer Sequences*, published electronically at http://oeis.org, 2014.
[4] D. J. Grabiner, P. Magyar. Random Walks in Weyl Chambers and the Decomposition of Tensor Powers. `http://math.msu.edu/~magyar/papers/RandomWalk.pdf`, 1993.