Algebra & Number Theory

Volume 9

2015

No. 1

Random matrices, the Cohen–Lenstra heuristics, and roots of unity

Derek Garton

msp

ALGEBRA AND NUMBER THEORY 9:1 (2015)
dx.doi.org/10.2140/ant.2015.9.149

Random matrices, the Cohen–Lenstra heuristics, and roots of unity

Derek Garton

The Cohen–Lenstra–Martinet heuristics predict the frequency with which a fixed finite abelian group appears as an ideal class group of an extension of number fields, for certain sets of extensions of a base field. Recently, Malle found numerical evidence suggesting that their proposed frequency is incorrect when there are unexpected roots of unity in the base field of these extensions. Moreover, Malle proposed a new frequency, which is a much better match for his data. We present a random matrix heuristic (coming from function fields) that leads to a function field version of Malle's conjecture (as well as generalizations of it).

1. Introduction

1.1. ***Cohen–Lenstra–Martinet and Malle.*** We start with Cohen and Lenstra's famous heuristic principle concerning the distribution of ideal class groups of quadratic number fields. We fix an odd prime ℓ, to be used throughout the paper.

Heuristic 1.1.1 [Cohen and Lenstra 1984]. A finite abelian ℓ-group should appear as the ℓ-Sylow subgroup of the ideal class group of an imaginary quadratic extension of $\mathbb{Q}$ with frequency inversely proportional to the order of its automorphism group.

With a bit more notation, we can reframe this heuristic. Let $\mathcal{G}$ be the poset of isomorphism classes of finite abelian ℓ-groups and for any number field K, let $\mathrm{cl}(K)$ denote the ideal class group of K. For any group G, let $G[\ell^\infty]$ denote its ℓ-Sylow subgroup. Now, since $\sum_{A\in\mathcal{G}} 1/|\mathrm{Aut}\,A| = \prod_{i=1}^{\infty}(1-\ell^{-i})^{-1}$ (a fact first proved by Hall [1938]), the map $\mathcal{G}\to\mathbb{R}$ given by $A\mapsto |\mathrm{Aut}\,A|^{-1}\prod_{i=1}^{\infty}(1-\ell^{-i})$ defines a discrete probability distribution on $\mathcal{G}$. Heuristic 1.1.1 is the claim that the statistics of this distribution match the statistics of ℓ-Sylow subgroups of imaginary quadratic extensions (when ordered by fundamental discriminant). In other words,

MSC2010: primary 11R29; secondary 11R58, 15B52.

Keywords: random matrices, function fields, roots of unity, ideal class groups, Cohen–Lenstra heuristics.

Heuristic 1.1.1 is equivalent to the following assertion: for any $A \in \mathcal{G}$,

$$\lim_{X\to\infty} \frac{\left|\{0 \le D \le X \mid -D \text{ a fundamental discriminant, } \operatorname{cl}(\mathbb{Q}(\sqrt{-D}))[\ell^\infty] \simeq A\}\right|}{\left|\{0 \le D \le X \mid -D \text{ a fundamental discriminant}\}\right|} = \frac{1}{|\operatorname{Aut} A|}\prod_{i=1}^{\infty}(1-\ell^{-i}).$$

(This assertion remains unproven; in fact, this limit is not even known to exist.) This heuristic explains many previously observed tendencies of class groups of imaginary quadratic fields; for example that their orders seem to be divisible by three with probability

$$1-\prod_{i=1}^{\infty}(1-3^{-i}) = \tfrac{1}{3}+\tfrac{1}{9}+\cdots \approx .44.$$

Cohen and Martinet [1990] extended their heuristics to include relative class groups of finite extensions of arbitrary number fields, placing different distributions on $\mathcal{G}$ depending on properties of the family of extensions they study. Once again, they proved that these distributions imply many numerical observations, thereby obtaining a new family of conjectures. (Recall that relative ideal class groups are defined as follows: if K/K_0 is an extension of number fields, the relative class group $\operatorname{cl}(K/K_0)$ is the kernel of the norm map $\mathrm{N}_{K/K_0} : \operatorname{cl}(K) \to \operatorname{cl}(K_0)$.)

However, Malle [2008] presented new computational data that called into question some of the Cohen–Lenstra–Martinet conjectures. For example, he studied the 3-parts of the relative class groups of quadratic extensions of $\mathbb{Q}(\sqrt{-3})$, which has third roots of unity. Cohen, Lenstra and Martinet predicted that the class numbers of such extensions should be coprime to 3 with probability

$$\prod_{i=2}^{\infty}(1-3^{-i}) \approx .840.$$

On the other hand, when Malle computed the class numbers of the first million of these extensions with discriminant at least 10^{20}, he discovered that the proportion of them with class number coprime to 3 was about .852. He conjectured that the proportion of all such class groups that have class number coprime to 3 should be exactly

$$\frac{4}{3}\prod_{i=1}^{\infty}(1+3^{-i})^{-1} \approx .852,$$

which is in much better agreement with his data. In a subsequent paper, Malle [2010] presented more computational evidence calling into question more of the Cohen–Lenstra–Martinet conjectures, once again when there are ℓth roots of unity in the base field. In that paper, he also presented a new family of distributions on $\mathcal{G}$ to describe relative class groups when the base field of the extension has ℓth roots of unity but not ℓ^2th roots of unity (see Conjecture 2.1 in [ibid.]). These distributions on $\mathcal{G}$ imply rank statistics that seem to be a much better fit for his new data. A special case of his conjecture is the following:

Conjecture 1.1.2 [Malle 2010]. Suppose that $A \in \mathcal{G}$ and that A has ℓ-rank r. Let K_0 be a number field with ℓth but not ℓ^2th roots of unity. Let $\mathcal{S}$ be the set of quadratic extensions K/K_0 with a fixed signature (with fixed relative unit rank u). Then

$$\lim_{X\to\infty} \frac{|\{K \in \mathcal{S} \mid |\mathrm{Disc}\, K| \le X, \mathrm{cl}(K/K_0)[\ell^\infty] \simeq A\}|}{|\{K \in \mathcal{S} \mid |\mathrm{Disc}\, K| \le X\}|} = \frac{\prod_{i=u+1}^{u+r} (\ell^i - 1)}{\ell^{r(u+1)}|A|^u |\mathrm{Aut}\, A|} \cdot \prod_{i=u+1}^{\infty} (1+\ell^{-i})^{-1}.$$

In this paper, we study a random matrix model of ideal class groups of function fields when the base field has ℓth roots of unity (i.e., the function field analog of the situation Malle studies in Conjecture 1.1.2). We compute the distributions on $\mathcal{G}$ given by this matrix model in two cases (see Theorem 5.1.4): in the case when the base field has ℓth roots of unity but not ℓ^2th roots of unity, and in the case when the base field has ℓ^2th roots of unity but not ℓ^3th roots of unity. In the former case, our distribution matches the distribution proposed by Malle. Moreover, we compute all the moments of the distribution given by this matrix model in the general case when the base case has ℓ^ξth but not $\ell^{\xi+1}$th roots of unity for any $\xi \in \mathbb{Z}^{>0}$ (see Corollary 3.2.7).

The work in this paper is based on my Ph.D. dissertation [Garton 2012]. The matrix distributions were computed independently in the Ph.D. dissertation of M. Adam [2014b] as well as in [Adam 2014a]. They are also used in [Adam and Malle 2015].

1.2. ***The function field case.*** Complementing the work described in Section 1.1, investigators have been studying analogous phenomena in function fields defined over finite fields. Friedman and Washington [1989] addressed the case of quadratic extensions of the field $\mathbb{F}_{p^n}(t)$ for a prime $p \neq 2$ and $n \in \mathbb{Z}^{>0}$. More precisely, if $f(t) \in \mathbb{F}_{p^n}[t]$ is monic of degree $2g+1$ with distinct roots, let C_f be the hyperelliptic curve (defined over $\mathbb{F}_{p^n}$) of genus g given by $y^2 = f(t)$. Note that the curve C_f has exactly one point at infinity, just as imaginary quadratic extensions of $\mathbb{Q}$ have exactly one place at infinity. Thus, $\mathrm{Pic}^0_{\mathbb{F}_{p^n}}(C_f)$ is isomorphic to the ideal class group of the field extension

$$\mathbb{F}_{p^n}(t)\big[\sqrt{f(t)}\,\big]/\mathbb{F}_{p^n}(t).$$

To study these groups, Friedman and Washington introduced a new heuristic principle, one that comes from the geometry of hyperelliptic curves over finite fields. Specifically, for $f(t) \in \mathbb{F}_{p^n}[t]$ monic of degree $2g+1$ with distinct roots, let $T_\ell(C_f)$ be the ℓ-adic Tate module of C_f, which is a free $2g$-dimensional $\mathbb{Z}_\ell$-module. In addition, let Frob_{p^n} be the p^n-power Frobenius map acting on $T_\ell(C_f)$. Thinking of Frob_{p^n} as a matrix over $\mathbb{Z}_\ell$, it is well known that $\mathrm{coker}(\mathrm{Id} - \mathrm{Frob}_{p^n})$ is isomorphic to the ℓ-Sylow subgroup of $\mathrm{Pic}^0_{\mathbb{F}_{p^n}}(C_f)$ (see the appendix of [Friedman and Washington 1989] for a proof of this fact). The same authors conjectured that the statistics of ℓ-Sylow subgroups of ideal class groups of quadratic extensions of $\mathbb{F}_{p^n}(t)$ match the statistics of ℓ-adic matrices. Specifically, if we let

$$F(g, p^n, \ell, A) :=$$
$$\frac{\bigl|\{f \in \mathbb{F}_{p^n}[t] \mid f \text{ monic with distinct roots, } \deg f{=}2g{+}1,\, \mathrm{Pic}^0_{\mathbb{F}_{p^n}}(C_f)[\ell^\infty] \simeq A\}\bigr|}{\bigl|\{f \in \mathbb{F}_{p^n}[t] \mid f \text{ monic with distinct roots, } \deg f = 2g+1\}\bigr|},$$

then they proposed the following:

Heuristic 1.2.1 [Friedman and Washington 1989]. If $A \in \mathcal{G}$, then

$$\lim_{g\to\infty} F(g, p^n, \ell, A) = \lim_{g\to\infty} \alpha_{2g}(\{\phi \in \mathrm{Mat}_{2g}(\mathbb{Z}_\ell) \mid \mathrm{coker}\,(\mathrm{Id} - \phi) \simeq A\}),$$

where α_{2g} is the normalized Haar measure on $\mathrm{Mat}_{2g}(\mathbb{Z}_\ell)$.

(See Sections 2.1 and 2.2 for more details on Haar measures.) Katz and Sarnak [1999] vastly extended the philosophy of considering the action of Frobenius as a random matrix, especially when the size of the base field is large. Friedman and Washington show that the limit on the right-hand side of Heuristic 1.2.1 exists, and that it defines exactly the same distribution on $\mathcal{G}$ as Cohen and Lenstra's original heuristic for imaginary quadratic extensions of $\mathbb{Q}$. However, just as the work of Malle calls into question the appropriateness of certain Cohen–Lenstra–Martinet distributions, it also calls into question the appropriateness of Friedman and Washington's proposed distribution. Indeed, the Friedman–Washington heuristic does not depend at all on the presence of ℓth roots of unity in the base field $\mathbb{F}_{p^n}(t)$, while Malle's work suggests that distributions modeling ℓ-Sylow subgroups of class groups ought to change in the presence of ℓth roots of unity. Thus, the new data of Malle suggests that Heuristic 1.2.1 might be flawed when $\mathbb{F}_{p^n}(t)$ has ℓth roots of unity.

A possible explanation for this flaw is that Frob_{p^n} is a symplectic similitude with respect to the Weil pairing on $T_\ell(C_f)$. Indeed, it scales the Weil pairing by p^n, so when considered as a matrix, $\mathrm{Frob}_{p^n} \in \mathrm{GSp}^{(p^n)}_{2g}(\mathbb{Z}_\ell)$. (See Section 2.1 for more details on this notation.) Since the presence of ℓth roots of unity in

$\mathbb{F}_{p^n}(t)$ depends on the congruence class of $p^n \pmod{\ell}$, the set of symplectic similitudes that scale the Weil pairing by p^n does indeed change when $\mathbb{F}_{p^n}(t)$ has ℓth roots of unity. These facts led Friedman and Washington (and Achter [2008]) to suggest:

Heuristic 1.2.2. If $A \in \mathcal{G}$, then

$$\lim_{g\to\infty} F(g, p^n, \ell, A) = \lim_{g\to\infty} \mu_{2g}^{(p^n)}(\{\phi \in \mathrm{GSp}_{2g}^{(p^n)}(\mathbb{Z}_\ell) \mid \operatorname{coker}(\mathrm{Id} - \phi) \simeq A\}),$$

where $\mu_{2g}^{(p^n)}$ is the unique normalized multiplicative Haar measure on $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ translated to $\mathrm{GSp}_{2g}^{(p^n)}(\mathbb{Z}_\ell)$.

(Again, see Sections 2.1 and 2.2 for more details on Haar measures.) Friedman and Washington hoped that this new heuristic would turn out to describe the same distribution as Heuristic 1.2.1, but Achter [2006] proved that

$$\lim_{g\to\infty} \mu_{2g}^{(p^n)}\big(\{\phi \in \mathrm{GSp}_{2g}^{(1)}(\mathbb{Z}_\ell) \mid \operatorname{coker}(\mathrm{Id} - \phi) \simeq \{0\}\}\big)$$
$$\neq \lim_{g\to\infty} \alpha_{2g}\big(\{\phi \in \mathrm{Mat}_{2g}(\mathbb{Z}_\ell) \mid \operatorname{coker}(\mathrm{Id} - \phi) \simeq \{0\}\}\big),$$

revealing that this was not the case, providing an early indication of the importance of the presence of ℓth roots of unity in the base field. Achter used work of Katz and Sarnak [1999] to prove a revised version of Heuristic 1.2.1:

Theorem 1.2.3 [Achter 2008]. *If $A \in \mathcal{G}$, then*

$$\lim_{p^n\to\infty} \big|F(g, p^n, \ell, A) - \mu_{2g}^{(p^n)}\big(\{\phi \in \mathrm{GSp}_{2g}^{(p^n)}(\mathbb{Z}_\ell) \mid \operatorname{coker}(\mathrm{Id} - \phi) \simeq A\}\big)\big| = 0.$$

We remark that this limit in Theorem 1.2.3 leaves g fixed while letting p^n increase, whereas the limit in Heuristic 1.2.2 does the opposite.

The work of Ellenberg, Venkatesh and Westerland [Ellenberg et al. 2009] uses the topology of Hurwitz spaces to study Heuristic 1.2.2. One consequence of their work is that

$$\lim_{g\to\infty} \lim_{\substack{p^n\to\infty \\ p^n \not\equiv 1 \pmod{\ell}}} F(g, p^n, \ell, A) = \frac{1}{|\mathrm{Aut}\, A|} \prod_{i=1}^{\infty} (1 - \ell^{-i}).$$

Since $p^n \equiv 1 \pmod{\ell}$ exactly when $\mathbb{F}_{p^n}(t)$ has ℓth roots of unity, this result only addresses the case when the base field does not have ℓth roots of unity (and only when $p^n \to \infty$). The remaining case is when $p^n \equiv 1 \pmod{\ell}$; that is, the case where there are ℓth roots of unity in the base field. Conjecture 1.1.2 suggests that a different distribution is needed to describe this case. In fact, Corollary 5.2.2 gives such a distribution. Using Achter's result (Theorem 1.2.3), Corollary 5.2.2 implies the following theorem:

Theorem 1.2.4. *If A is a finite abelian ℓ-group with ℓ-rank r and ℓ^2-rank s, then*

$$\lim_{g\to\infty} \lim_{\substack{p^n\to\infty \\ p^n\equiv 1 \pmod{\ell^\xi}, \\ p^n\not\equiv 1 \pmod{\ell^{\xi+1}}}} F(g, p^n, \ell, A)$$

$$= \begin{cases} \ell^{\frac{r(r-1)}{2}} \cdot (\ell^{-1}; \ell^{-1})_r \cdot \dfrac{\prod_{i=1}^{\infty} (1+\ell^{-i})^{-1}}{|\operatorname{Aut} A|^{-1}} & \text{if } \xi = 1, \\ \ell^{\frac{r(r-1)}{2}+\frac{s(s-1)}{2}} \cdot (\ell^{-1}; \ell^{-1})_s \cdot (\ell^{-1}; \ell^{-2})_{\lceil\frac{r-s}{2}\rceil} \cdot \dfrac{\prod_{i=1}^{\infty} (1+\ell^{-i})^{-1}}{|\operatorname{Aut} A|^{-1}} & \text{if } \xi = 2, \end{cases}$$

where $(\ell^{-1}; \ell^{-j})_k$ is the ℓ^{-j}-Pochhammer symbol, defined for any $j \in \mathbb{Z}^{>0}$ and $k \in \mathbb{Z}^{\geq 0}$ (see Notation 5.1.1).

Theorem 1.2.4 extends Conjecture 1.1.2 by including the case where $\mathbb{F}_{p^n}(t)$ has ℓ^2th roots of unity but not ℓ^3th roots of unity. Since imaginary hyperelliptic curves have only one place at infinity, the function field version of Conjecture 1.1.2 should set $u = 0$; making this substitution in Conjecture 1.1.2 yields the $\xi = 1$ case of Theorem 1.2.4.

2. Preliminaries

2.1. ***Notation and definitions.*** As above, let ℓ be an odd prime and let $\mathscr{G}$ be the poset of isomorphism classes of finite abelian ℓ-groups, with the relation $[A] \leq [B]$ if and only if there exists an injection $A \hookrightarrow B$. (For notational simplicity, we will conflate finite abelian ℓ-groups and the equivalence classes containing them.) For any $A \in \mathscr{G}$, we denote the exponent of A by $\exp A$. If $i \in \mathbb{Z}^{>0}$, let

$$\operatorname{rank}_{\ell^i} A := \dim_{\mathbb{F}_\ell}(\ell^{i-1}A/\ell^i A).$$

We will abbreviate $\operatorname{rank}_\ell A$ by $\operatorname{rank} A$. If $r_1, \ldots, r_{i-1} \in \mathbb{Z}^{>0}$ and $r_i \in \mathbb{Z}^{\geq 0}$, let $\mathscr{G}(r_1, \ldots, r_i)$ be the following subposet of $\mathscr{G}$:

$$\mathscr{G}(r_1, \ldots, r_i) := \{A \in \mathscr{G} \mid \operatorname{rank}_{\ell^j} A = r_j \text{ for all } j \in \{1, \ldots, i\}\}.$$

Next, for any $\rho \in \mathbb{Z}^{>0}$, set $R_\rho = \mathbb{Z}_\ell/\ell^\rho\mathbb{Z}_\ell \simeq \mathbb{Z}/\ell^\rho\mathbb{Z}$. For any $g, \rho \in \mathbb{Z}^{>0}$, let $\langle\,\cdot\,,\cdot\,\rangle_{2g,\rho}$ be the symplectic form on $(R_\rho)^{2g}$ given by

$$\Omega_g := \begin{pmatrix} 0 & \operatorname{Id}_g \\ -\operatorname{Id}_g & 0 \end{pmatrix}$$

with respect to the standard basis; note that $\langle\,\cdot\,,\cdot\,\rangle_{2g,a} : (R_\rho)^{2g} \times (R_\rho)^{2g} \to (R_\rho)$ is R_ρ-bilinear, alternating and nondegenerate. (See Theorem III.2 of [McDonald 1976] for more details on symplectic spaces.) Let $\langle\,\cdot\,,\cdot\,\rangle_{2g}$ be the analogous choice of symplectic form on $(\mathbb{Z}_\ell)^{2g}$. For any ring R and any $g \in \mathbb{Z}^{>0}$, if R^{2g} has a symplectic form $\langle\,\cdot\,,\,\cdot\,\rangle$, then the *symplectic group of R* is

$$\begin{aligned}\mathrm{Sp}_{2g}(R) &\simeq \mathrm{Sp}(R^{2g}, \langle\,\cdot\,,\,\cdot\,\rangle)\\ &= \{\phi \in \mathrm{GL}(R^{2g}) \mid \langle \phi(\boldsymbol{x}), \phi(\boldsymbol{y})\rangle = \langle \boldsymbol{x}, \boldsymbol{y}\rangle \text{ for all } \boldsymbol{x}, \boldsymbol{y} \in R^{2g}\}.\end{aligned}$$

Note that a different choice of symplectic form on R^{2g} yields an isometric space, so the choice is immaterial (see p. 188 of [McDonald 1976] for more details). Similarly, the *group of symplectic similitudes of R* is

$$\begin{aligned}\mathrm{GSp}_{2g}(R) \simeq \mathrm{GSp}(R^{2g}, \langle\,\cdot\,,\,\cdot\,\rangle) = \big\{\phi \in \mathrm{GL}(R^{2g}) \mid \text{there exists } m(\phi) \in R^{\times}\\ \text{such that } \langle \phi(\boldsymbol{x}), \phi(\boldsymbol{y})\rangle = m(\phi)\cdot\langle \boldsymbol{x}, \boldsymbol{y}\rangle \text{ for all } \boldsymbol{x}, \boldsymbol{y} \in R^{2g}\big\}.\end{aligned}$$

For concreteness, we will always assume that the rings $(R_\rho)^{2g}$ and $(\mathbb{Z}_\ell)^{2g}$ are equipped with the forms $\langle\,\cdot\,,\,\cdot\,\rangle_{2g,\rho}$ and $\langle\,\cdot\,,\,\cdot\,\rangle_{2g}$ fixed above. The map

$$m : \mathrm{GSp}_{2g}(R) \to R^{\times} : \phi \mapsto m(\phi)$$

described above is a homomorphism called the *multiplier map*, and the element $m(\phi) \in R^{\times}$ is called the *multiplier* of ϕ. For any $g \in \mathbb{Z}^{>0}$, let μ_{2g} be the unique Haar measure on $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ satisfying $\mu_{2g}(\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)) = 1$. (We say a Haar measure satisfying this last condition is *normalized*.) Note that μ_{2g} is invariant under both left and right multiplication since $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ is a unimodular group. Finally, for any $g \in \mathbb{Z}^{>0}$ and any unit x in a ring R, let $\mathrm{GSp}^{(x)}_{2g}(R) = m^{-1}(x)$.

For any $x \in (\mathbb{Z}_\ell)^{\times}$ and $\phi \in \mathrm{GSp}^{(x)}_{2g}(\mathbb{Z}_\ell)$ we define a measure $\mu^{(x)}_{2g}$ on $\mathrm{GSp}^{(x)}_{2g}(\mathbb{Z}_\ell)$ as follows: for any μ_{2g}-measurable subset $S \subseteq \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$, define

$$\mu^{(x)}_{2g}(S\phi) := \mu_{2g}(S).$$

This measure is independent of the choice $\phi \in \mathrm{GSp}^{(x)}_{2g}(\mathbb{Z}_\ell)$. Indeed, given some other $\psi \in \mathrm{GSp}^{(x)}_{2g}(\mathbb{Z}_\ell)$, there exists a unique $\phi_\psi \in \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ such that $\phi_\psi\phi = \psi$; i.e., $S\psi = S\phi_\psi\phi$. Since μ_{2g} is translation-invariant, we know that

$$\mu_{2g}(S) = \mu_{2g}(S\phi_\psi),$$

as desired. Moreover, since μ_{2g} is translation-invariant (by $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$) and normalized, so is $\mu^{(x)}_{2g}$. Similarly, for any $\rho \in \mathbb{Z}^{>0}$, let $\nu_{2g,\rho}$ be the unique normalized Haar measure on $\mathrm{Sp}_{2g}(R_\rho)$, and for any $x \in R^{\times}_\rho$, define $\nu^{(x)}_{2g,\rho}$ on $\mathrm{GSp}^{(x)}_{2g}(R_\rho)$ as above. For any $\rho \in \mathbb{Z}^{>0}$, $x \in R^{\times}_\rho$ and $S \subseteq \mathrm{GSp}^{(x)}_{2g}(R_\rho)$, we know $\nu^{(x)}_{2g,\rho}(S) = |S|\cdot|\mathrm{Sp}_{2g}(R_\rho)|^{-1}$, since $\mathrm{Sp}_{2g}(R_\rho)$ is a finite group. To ease notation, for any $A \in \mathscr{G}$, $g \in \mathbb{Z}^{>0}$ and $x \in (\mathbb{Z}_\ell)^{\times}$, we set

$$\mu^{(x)}_{2g}(A) := \mu^{(x)}_{2g}(\{\phi \in \mathrm{GSp}^{(x)}_{2g}(\mathbb{Z}_\ell) \mid \mathrm{coker}(\mathrm{Id} - \phi) \simeq A\}).$$

Furthermore, if $\rho \in \mathbb{Z}^{>0}$ and $x \in R_\rho^\times$, set

$$\nu_{2g,\rho}^{(x)}(A) := \nu_{2g,\rho}^{(x)}(\{\gamma \in \mathrm{GSp}_{2g}^{(x)}(R_\rho) \mid \operatorname{coker}(\mathrm{Id} - \gamma) \simeq A\}).$$

2.2. ***The Haar measures.*** The measures defined in Section 2.1 have an important relationship, given in the following lemma.

Lemma 2.2.1. *Suppose $A \in \mathcal{G}$, $g \in \mathbb{Z}^{>0}$, $x \in (\mathbb{Z}_\ell)^\times$ and $\rho \in \mathbb{Z}^{>0}$. Let $\overline{\cdot} : \mathbb{Z}_\ell \to R_\rho$ denote reduction mod ℓ^ρ. If $\ell^\rho > \exp A$, then*

$$\mu_{2g}^{(x)}(A) = \nu_{2g,\rho}^{(\bar{x})}(A).$$

Proof. Choose any $\phi \in \mathrm{GSp}_{2g}^{(x)}(\mathbb{Z}_\ell)$. Then for any measurable $S \subseteq \mathrm{GSp}_{2g}^{(x)}(\mathbb{Z}_\ell)$, we know that

$$\mu_{2g}^{(x)}(S) = \mu_{2g}^{(x)}(S\phi^{-1}\phi) = \mu_{2g}(S\phi^{-1})$$

by the definition of $\mu_{2g}^{(x)}$. Since μ_{2g} is invariant under translation, every coset of the kernel of the reduction map $\overline{\cdot} : \mathrm{Sp}_{2g}(\mathbb{Z}_\ell) \to R_\rho$ has the same measure; namely,

$$[\mathrm{Sp}_{2g}(\mathbb{Z}_\ell) : \ker(\overline{\cdot})]^{-1} = |\mathrm{Sp}_{2g}(R_\rho)|^{-1}.$$

Moreover, note that if $\psi \in \mathrm{GSp}_{2g}^{(x)}(\mathbb{Z}_\ell)$, then $m(\bar{\psi}) = \overline{m(\psi)}$ and $\operatorname{coker}(\mathrm{Id} - \psi) \simeq A$ if and only if $\operatorname{coker}(\mathrm{Id} - \bar{\psi}) \simeq A$, since $\ell^\rho > \exp A$. The result follows. □

Notation 2.2.2. Suppose that $g \in \mathbb{Z}^{>0}$ and $\xi \in \mathbb{Z}^{\geq 0}$. For $\rho \in \mathbb{Z}^{>0}$ satisfying $\rho \geq \xi$, we define an important subgroup of $\mathrm{GSp}_{2g}(R_\rho)$:

$$\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho) := \{\gamma \in \mathrm{GSp}_{2g}(R_\rho) \mid m(\gamma) \in \ell^\xi R_\rho + 1\}.$$

Note that $\mathrm{GSp}_{2g}^{\langle\rho\rangle}(R_\rho) = \mathrm{Sp}_{2g}(R_\rho)$ and $\mathrm{GSp}_{2g}^{\langle 0\rangle}(R_\rho) = \mathrm{GSp}_{2g}(R_\rho)$. For any $A \in \mathcal{G}$, we adopt the suggestive notation

$$N_{2g,\rho}^{\langle\xi\rangle}(A) := |\{\gamma \in \mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho) \mid \operatorname{coker}(\mathrm{Id} - \gamma) \simeq A\}|$$

and, if $\rho > \xi$,

$$\nu_{2g,\rho}^{\langle\xi\rangle}(A) := \frac{N_{2g,\rho}^{\langle\xi\rangle}(A) - N_{2g,\rho}^{\langle\xi+1\rangle}(A)}{|\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)| - |\mathrm{GSp}_{2g}^{\langle\xi+1\rangle}(R_\rho)|}.$$

Goal 2.2.3. We can now state the matrix-theoretic analog of the situation about which Malle made his Conjecture 2.1. Following Heuristic 1.2.2, for $A \in \mathcal{G}$, $x \in (\mathbb{Z}_\ell)^\times$ and $\xi \in \mathbb{Z}^{>0}$, with $x \equiv 1 \pmod{\ell^\xi}$ but $x \not\equiv 1 \pmod{\ell^{\xi+1}}$, we must evaluate

$$\mu_x(A) := \lim_{g\to\infty} \mu_{2g}^{(x)}(A).$$

If we let $\bar{\cdot} : \mathbb{Z}_\ell \to R_\rho$ denote reduction mod ℓ^ρ, then we know by Lemma 2.2.1 that this amounts to calculating

$$\lim_{g\to\infty} \nu_{2g,\rho}^{(\bar{x})}(A)$$

for any $\rho \in \mathbb{Z}^{>0}$ satisfying both $\ell^\rho > \exp A$ and $\rho > \xi$. In Note 3.1.5 we will see that, for all such ρ,

$$\nu_{2g,\rho}^{(\bar{x})}(A) = \nu_{2g,\rho}^{\langle\xi\rangle}(A),$$

so we will turn our attention to computing

$$\lim_{g\to\infty} \nu_{2g,\rho}^{\langle\xi\rangle}(A),$$

which we compute explicitly for $\xi = 1, 2$ in Corollary 5.2.2. Using Achter's result, Theorem 1.2.3, we then obtain Theorem 1.2.4 as a corollary.

Remark 2.2.4. Suppose that $x \in \mathbb{Z}_\ell$. In addition to explicitly computing the distribution $\mu_x : \mathcal{G} \to \mathbb{R}$ if $x \equiv 1 \pmod{\ell^\xi}$ but $x \not\equiv 1 \pmod{\ell^{\xi+1}}$ for $\xi = 1, 2$, we also compute the moments of this distribution for any $\xi \in \mathbb{Z}^{>0}$. Specifically, in Corollary 3.2.7 we find that if $A \in \mathcal{G}$ then

$$\sum_{B\in\mathcal{G}} |\mathrm{Surj}(B, A)|\,\mu_x(B) = |\Lambda(A/\ell^\xi)|.$$

(See Notation 3.2.1 for the definition of Λ.) For any $A \in \mathcal{G}$, we call the quantity $\sum_{B\in\mathcal{G}} |\mathrm{Surj}(B, A)|\mu_x(B)$ the "Ath moment" of the distribution μ_x by analogy. Just as the kth moment of a real-valued random variable X is the expected value of X^k, the Ath moment of μ_x is the expected value of $|\mathrm{Surj}(B, A)|$, where B is a $\mathcal{G}$-valued random variable. Moreover, under certain favorable conditions, the set of Ath moments of a distribution on $\mathcal{G}$ determines the distribution, making the analogy even stronger. The term "Ath moment" is becoming standard in the literature related to the Cohen–Lenstra heuristics (see, for example, [Ellenberg et al. 2009; Matchett Wood 2014]).

3. The symplectic action

3.1. *Basic properties.*

Notation 3.1.1. For any $A, B \in \mathcal{G}$, let $\mathrm{Inj}(A, B)$ and $\mathrm{Surj}(A, B)$ be the sets of injective homomorphisms and surjective homomorphisms from A to B.

In what follows, we will consider either injections or surjections (as well as either kernels or cokernels) depending on which is more convenient at the time. The next two lemmas justify this shifting point of view.

Lemma 3.1.2. *Suppose that $A \in \mathscr{G}$, $g, \rho \in \mathbb{Z}^{>0}$ and $\xi \in \mathbb{Z}^{\geq 0}$. If $\rho \geq \xi$, then* $\mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho)$ *acts on* $\mathrm{Inj}(A, (R_\rho)^{2g})$ *and* $\mathrm{Surj}((R_\rho)^{2g}, A)$ *by postcomposition and precomposition, respectively. These actions have the same number of orbits.*

Proof. If $\ell^\rho < \exp A$, the result is trivial, so suppose $\ell^\rho \geq \exp A$. In this case, we can think of A as an R_ρ-module. Moreover, we know that R_ρ is an injective R_ρ-module by Baer's criterion, so the functor

$$(\,\cdot\,)^\vee := \mathrm{Hom}(\,\cdot\,, R_\rho) : R_\rho\mathtt{-mod} \to R_\rho\mathtt{-mod}$$

is exact. Thus, for any $\gamma \in \mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho)$,

$$f, h \in \mathrm{Inj}(A, (R_\rho)^{2g}) \quad \text{with } \gamma \circ f = h$$

if and only if

$$f^\vee, h^\vee \in \mathrm{Surj}(((R_\rho)^{2g})^\vee, A^\vee) \quad \text{with } f^\vee \circ \gamma^\vee = h^\vee.$$

After choosing R_ρ-bases for $(R_\rho)^{2g}$ and A, it is easy to see that $((R_\rho)^{2g})^\vee \simeq (R_\rho)^{2g}$, $A^\vee \simeq A$ and $\gamma^\vee = \gamma^\top \in \mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho)$, giving the result. □

The number orbits of the action described above turn out to be very important, so we bestow a name upon them:

Definition 3.1.3. Suppose that $A \in \mathscr{G}$, $g, \rho \in \mathbb{Z}^{>0}$ and $\xi \in \mathbb{Z}^{\geq 0}$. If $\rho \geq \xi$, let $o_{2g,\rho}^{A,\langle \xi \rangle}$ be the number of orbits of $\mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho)$ acting on $\mathrm{Inj}(A, (R_\rho)^{2g})$ or $\mathrm{Surj}((R_\rho)^{2g}, A)$.

Lemma 3.1.4. *For A, g, ρ, ξ as above,*

$$N_{2g,\rho}^{\langle \xi \rangle}(A) = \left|\{\gamma \in \mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho) \mid \ker(\mathrm{Id} - \gamma) \simeq A\}\right|.$$

Proof. As in Lemma 3.1.2, this follows from the exactness of $(\,\cdot\,)^\vee$. Note that, for any $\gamma \in \mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho)$,

$$(\mathrm{coker}(\mathrm{Id} - \gamma))^\vee = \ker((\mathrm{Id} - \gamma)^\vee) = \ker(\mathrm{Id} - \gamma^\top),$$

giving the result. □

In Goal 2.2.3, we turned our attention from the measures of cosets of the symplectic group to subgroups of the group of symplectic similitudes. The following note justifies this turn.

Note 3.1.5. Suppose that $A \in \mathscr{G}$, $g \in \mathbb{Z}^{>0}$, $x \in \mathbb{Z}_\ell$ and $\xi \in \mathbb{Z}^{>0}$, with $x \equiv 1 \pmod{\ell^\xi}$ but $x \not\equiv 1 \pmod{\ell^{\xi+1}}$. If $\rho \in \mathbb{Z}^{>0}$ satisfies $\rho > \xi$, then

$$\nu_{2g,\rho}^{(\bar{x})}(A) = \nu_{2g,\rho}^{\langle \xi \rangle}(A).$$

Proof. This amounts to showing that if $x, y \in R_\rho$ such that $x \equiv y \equiv 1 \pmod{\ell^\xi}$ but neither x nor y is equivalent to $1 \pmod{\ell^{\xi+1}}$, then

$$\nu_{2g,\rho}^{(\bar{x})}(A) = \nu_{2g,\rho}^{(\bar{y})}(A).$$

By our assumptions on x and y, there exists some m_0 such that $\ell \nmid m_0$ and $\bar{x}^{m_0} = \bar{y}$. Choose some m in the arithmetic progression $\{m_0 + \ell^{\rho-\xi} j\}_{j=0}^{\infty}$ such that

$$\gcd(m, |\mathrm{GSp}_{2g}(R_\rho)|) = 1,$$

and choose k such that $mk \equiv 1 \pmod{|\mathrm{GSp}_{2g}(R_\rho)|}$. Now, the map

$$\begin{aligned} (\,\cdot\,)^m : \mathrm{GSp}_{2g}^{(\bar{x})}(R_\rho) &\to \mathrm{GSp}_{2g}^{(\bar{y})}(R_\rho) \\ \gamma &\mapsto \gamma^m \end{aligned}$$

is bijective with inverse $(\,\cdot\,)^k$. Moreover, for any $z \in (R_\rho)^{2g}$ and any $\gamma \in \mathrm{GSp}_{2g}^{(\bar{x})}(R_\rho)$, it is clear that $\gamma z = z$ if and only if $\gamma^m z = z$. Thus, we obtain

$$\left|\{\gamma \in \mathrm{GSp}_{2g}^{(\bar{x})}(R_\rho) \mid \ker(\mathrm{Id} - \gamma) \simeq A\}\right| = \left|\{\gamma \in \mathrm{GSp}_{2g}^{(\bar{y})}(R_\rho) \mid \ker(\mathrm{Id} - \gamma) \simeq A\}\right|,$$

and we conclude by Lemma 3.1.4. □

3.2. *Orbit counting.*

Notation 3.2.1. For any $A \in \mathcal{G}$, let $\Lambda(A)$ be the set of alternating bilinear forms on A thought of as a $(\mathbb{Z}/\exp A)$-module.

Note 3.2.2. Suppose that $A = \mathbb{Z}/\ell^{\alpha_1} \oplus \cdots \oplus \mathbb{Z}/\ell^{\alpha_r}$ with $\alpha_1 \geq \cdots \geq \alpha_r > 0$. Then

$$|\Lambda(A)| = \ell^{\sum_{i=2}^{r} (i-1)\alpha_i}$$

Proof. Let $\{\boldsymbol{e}_i\}_{i=1}^r$ be a $(\mathbb{Z}/\exp A)$-basis for A such that $\boldsymbol{e}_i$ has order ℓ^{α_i} for all $i \in \{1, \dots, r\}$. Every alternating bilinear form $\langle\,\cdot\,,\cdot\,\rangle$ on A corresponds to an antisymmetric matrix $(\langle \boldsymbol{e}_i, \boldsymbol{e}_j\rangle) \in \mathrm{Mat}_{r\times r}(\mathbb{Z}/\exp A)$. Moreover, $\ell^{\alpha_j}\langle \boldsymbol{e}_i, \boldsymbol{e}_j\rangle = \langle \boldsymbol{e}_i, \ell^{\alpha_j}\boldsymbol{e}_j\rangle = 0$ for all $i < j$ since $\boldsymbol{e}_i$ has order ℓ^{α_i} for all $i \in \{1, \dots, r\}$. Conversely, any antisymmetric matrix $(a_{ij}) \in \mathrm{Mat}_{r\times r}(\mathbb{Z}/\exp A)$ corresponds to an alternating bilinear form on A, as long it has 0s along its main diagonal and $\ell^{\alpha_j} a_{ij} = 0$ whenever $i < j$ (this requirement encodes the fact that any bilinear form $\langle\,\cdot\,,\cdot\,\rangle$ on A must satisfy $\ell^{\alpha_j}\langle \boldsymbol{e}_i, \boldsymbol{e}_j\rangle = 0$ for all $i < j$). There are ℓ^{α_j} such elements of $\mathbb{Z}/\exp A$, so the result follows. □

Lemma 3.2.3. *Suppose that $r \in \mathbb{Z}^{\geq 0}$, $A \in \mathcal{G}(r)$, $g, \rho \in \mathbb{Z}^{>0}$ and $\xi \in \mathbb{Z}^{\geq 0}$. If $\ell^\rho \geq \exp A$, $\rho \geq \xi$ and $2g \geq r$, then*

$$o_{2g,\rho}^{A,\langle\xi\rangle} \leq \ell^{-(\rho-\xi)}|\Lambda(A)| + (\ell - 1)\sum_{i=0}^{\rho-\xi-1} \ell^{-(i+1)}|\Lambda(A/\ell^{\xi+i})|.$$

Furthermore, when $g \geq r$, the upper bound above is an equality. (*In particular, $o_{2g,\rho}^{A,\langle\xi\rangle}$ is independent of g for large enough g.*)

As pointed out in Goal 2.2.3, we need only calculate

$$\lim_{g\to\infty} \nu_{2g,\rho}^{\langle\xi\rangle}(A).$$

Despite this fact, the inequality for small g in Lemma 3.2.3 does indeed turn out to be useful. This is due to the fact that $\nu_{2g,\rho}^{\langle\xi\rangle}(A)$ can be expressed as a sum of orbit data for finite abelian groups of rank up to $2g$. (See Corollary 4.2.4.)

Proof of the lemma. The result is obviously true when $r = 0$, so suppose that $r > 0$. Theorem 2.14 of [Michael 2006] shows that the set of orbit representatives of $\mathrm{GSp}_{2g}^{\langle\rho\rangle}(R_\rho) = \mathrm{Sp}_{2g}(R_\rho)$ acting on $\mathrm{Surj}((R_\rho)^{2g}, A)$ injects into $\Lambda(A)$; there, this injection is denoted s', and when $g \geq r$, the map s' is a bijection.

We can define an action of $(R_\rho)^\times = \mathrm{GSp}_{2g}(R_\rho)/\mathrm{Sp}_{2g}(R_\rho)$ on $\mathrm{Surj}((R_\rho)^{2g}, A)$ as follows. For any $x \in (R_\rho)^\times$ and $f \in \mathrm{Surj}((R_\rho)^{2g}, A)$, note that

$$\begin{pmatrix} 0 & x\cdot\mathrm{Id}_g \\ -\mathrm{Id}_g & 0 \end{pmatrix} \in \mathrm{GSp}_{2g}(R_\rho), \quad \text{and define} \quad x\cdot f = f \circ \begin{pmatrix} 0 & x\cdot\mathrm{Id}_g \\ -\mathrm{Id}_g & 0 \end{pmatrix}.$$

We can also define an action of $(R_\rho)^\times$ on $\Lambda(A)$ by $x \cdot \langle\cdot,\cdot\rangle = x\langle\cdot,\cdot\rangle$ for any $x \in (R_\rho)^\times$ and $\langle\cdot,\cdot\rangle \in \Lambda(A)$. Again referring to the notation of [ibid.], the map s' is equivariant with respect to these two actions. (This follows from the definition of the map s' and the comment immediately preceding Lemma 2.2 from [ibid.].)

Thus, computing the number of orbits of $\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)$ acting on $\mathrm{Surj}((R_\rho)^{2g}, A)$ is a straightforward application of Burnside's counting theorem. Indeed, suppose that $A = \mathbb{Z}/\ell^{\alpha_1} \oplus \cdots \oplus \mathbb{Z}/\ell^{\alpha_r}$ with $\alpha_1 \geq \cdots \geq \alpha_r > 0$, then use Note 3.2.2 to see that

$$\begin{aligned}
o_{2g,\rho}^{A,\langle\xi\rangle} &\leq \frac{1}{|\ell^\xi R_\rho + 1|} \cdot \sum_{\upsilon\in\ell^\xi R_\rho+1} |\mathrm{Fix}\,(\upsilon)| \\
&= \frac{1}{|\ell^\xi R_\rho + 1|}\Bigg(\Bigg(\sum_{i=0}^{\rho-\xi-1} \sum_{\upsilon\in(\ell^{\xi+i}R_\rho+1)\setminus(\ell^{\xi+i+1}R_\rho+1)} |\mathrm{Fix}(\upsilon)|\Bigg) + \sum_{\upsilon\in\ell^\rho R_\rho+1=\{1\}} |\mathrm{Fix}(\upsilon)|\Bigg) \\
&= \frac{1}{\ell^{\rho-\xi}}\Bigg(\sum_{i=0}^{\rho-\xi-1} (\ell^{\rho-\xi-i} - \ell^{\rho-\xi-i-1})\ell^{\sum_{j=2}^{r}(j-1)\min\{\xi+i,\alpha_j\}} + \ell^{\alpha_2+2\alpha_3+\cdots+(r-1)\alpha_r}\Bigg) \\
&= \frac{1}{\ell^{\rho-\xi}}|\Lambda(A)| + (\ell-1)\sum_{i=0}^{\rho-\xi-1} \ell^{-(i+1)}|\Lambda(A/\ell^{\xi+i})|,
\end{aligned}$$

with equality when $g \geq r$. □

Notation 3.2.4. Suppose that $A \in \mathcal{G}$, $\rho \in \mathbb{Z}^{>0}$ and $\xi \in \mathbb{Z}^{\geq 0}$. If $\ell^\rho \geq \exp A$ and $\rho \geq \xi$, use Lemma 3.2.3 to define $o_\rho^{A,\langle\xi\rangle} := o_{2g,\rho}^{A,\langle\xi\rangle}$ for any $g \in \mathbb{Z}^{>0}$ such that $g \geq \operatorname{rank} A$.

We now mention an identity which will be useful later. (See Corollary 3.2.7 and Note 4.2.5.)

Note 3.2.5. Suppose $A \in \mathcal{G}$ and $\rho, \xi \in \mathbb{Z}^{>0}$. If $\ell^\rho \geq \exp A$ and $\rho > \xi$, then by Lemma 3.2.3 and Note 3.2.2, we see that

$$\ell o_\rho^{A,\langle\xi\rangle} - o_\rho^{A,\langle\xi+1\rangle} = (\ell - 1)|\Lambda(A/\ell^\xi)|.$$

Below is a simple observation, which has Corollary 3.2.7 as an important consequence. This corollary gives the moments of the probability distributions $\mu_x : \mathcal{G} \to \mathbb{R}$ for any $x \in \mathbb{Z}_\ell$, as promised in Section 2.2.

Lemma 3.2.6. *Suppose that $A \in \mathcal{G}$, $g, \rho \in \mathbb{Z}^{>0}$ and $\xi \in \mathbb{Z}^{\geq 0}$. Furthermore, suppose $\rho \geq \xi$, let $\gamma \in \mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)$, and consider $\mathrm{Inj}(A, \ker(\mathrm{Id} - \gamma)) \subseteq \mathrm{Inj}(A, (R_\rho)^{2g})$. There is a one-to-one correspondence between $\mathrm{Inj}(A, \ker(\mathrm{Id} - \gamma))$ and $\mathrm{Fix}(\gamma)$. Dually, there is a one-to-one correspondence between $\mathrm{Surj}(\mathrm{coker}(\mathrm{Id} - \gamma), A)$ and $\mathrm{Fix}(\gamma)$.*

Proof. Suppose that $f \in \mathrm{Inj}(A, (R_\rho)^{2g})$. Note that $f \in \mathrm{Inj}(A, \ker(\mathrm{Id} - \gamma))$ if and only if $(\mathrm{Id} - \gamma) f = 0$ if and only if $f = \gamma f$. The dual proof is similar. □

Corollary 3.2.7. *Let $x \in \mathbb{Z}_\ell$ and suppose that $x \equiv 1 \pmod{\ell^\xi}$ but $x \not\equiv 1 \pmod{\ell^{\xi+1}}$ for some $\xi \in \mathbb{Z}^{>0}$. If $A \in \mathcal{G}$, then*

$$\sum_{B \in \mathcal{G}} |\mathrm{Surj}(B, A)| \mu_x(B) = |\Lambda(A/\ell^\xi)|.$$

Proof. Choose any $g, \rho \in \mathbb{Z}^{>0}$ such that $g \geq \operatorname{rank} A$, $\ell^\rho \geq \exp A$, and $\rho > \xi$. To begin with, note that

$$\begin{aligned}
&\sum_{B \in \mathcal{G}} |\mathrm{Surj}(B, A)| \nu_{2g,\rho}^{(x)}(B) \\
&\quad = |\mathrm{GSp}_{2g}^{(x)}(R_\rho)|^{-1} \cdot \sum_{B \in \mathcal{G}} |\mathrm{Surj}(B, A)| \cdot \left|\{\gamma \in \mathrm{GSp}_{2g}^{(x)}(R_\rho) \mid \mathrm{coker}(\mathrm{Id} - \gamma) \simeq B\}\right| \\
&\quad = |\mathrm{GSp}_{2g}^{(x)}(R_\rho)|^{-1} \cdot \sum_{\gamma \in \mathrm{GSp}_{2g}^{(x)}(R_\rho)} |\mathrm{Surj}(\mathrm{coker}(\mathrm{Id} - \gamma), A)|.
\end{aligned}$$

Now, thanks to Note 3.1.5, we can turn our attention to the quantity

$$|\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho) \setminus \mathrm{GSp}_{2g}^{\langle\xi+1\rangle}(R_\rho)|^{-1} \cdot \sum_{\gamma \in \mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho) \setminus \mathrm{GSp}_{2g}^{\langle\xi+1\rangle}(R_\rho)} |\mathrm{Surj}(\mathrm{coker}(\mathrm{Id} - \gamma), A)|.$$

Using the fact that $|\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)| = \ell |\mathrm{GSp}_{2g}^{\langle\xi+1\rangle}(R_\rho)|$ and applying Lemma 3.2.6 to $\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)$ acting on $\mathrm{Surj}((R_\rho)^{2g}, A)$, then using Burnside's counting theorem and Notation 3.2.4, we see that

$$\begin{aligned}
&|\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)\setminus\mathrm{GSp}_{2g}^{\langle\xi+1\rangle}(R_\rho)|^{-1}\cdot\sum_{\gamma\in\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)\setminus\mathrm{GSp}_{2g}^{\langle\xi+1\rangle}(R_\rho)}|\mathrm{Surj}(\mathrm{coker}(\mathrm{Id}-\gamma),\,A)|\\
&\quad=\frac{\ell}{(\ell-1)\,|\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)|}\biggl(\sum_{\gamma\in\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)}|\mathrm{Fix}\,\gamma|-\sum_{\gamma\in\mathrm{GSp}_{2g}^{\langle\xi+1\rangle}(R_\rho)}|\mathrm{Fix}\,\gamma|\biggr)\\
&\quad=\frac{\ell}{\ell-1}\biggl(\sum_{\gamma\in\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)}\frac{|\mathrm{Fix}\,\gamma|}{|\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)|}-\sum_{\gamma\in\mathrm{GSp}_{2g}^{\langle\xi+1\rangle}(R_\rho)}\frac{|\mathrm{Fix}\,\gamma|}{\ell\,|\mathrm{GSp}_{2g}^{\langle\xi+1\rangle}(R_\rho)|}\biggr)\\
&\quad=\frac{\ell}{\ell-1}\biggl(o_{2g,\rho}^{A,\langle\xi\rangle}-\frac{1}{\ell}o_{2g,\rho}^{A,\langle\xi+1\rangle}\biggr)\\
&\quad=\frac{1}{\ell-1}\bigl(\ell o_{\rho}^{A,\langle\xi\rangle}-o_{\rho}^{A,\langle\xi+1\rangle}\bigr),
\end{aligned}$$

so we can conclude by applying Note 3.2.5 and Lemma 2.2.1. □

4. A weighted Möbius function

4.1. ***First observations.*** Let $\mathcal{P}$ be a locally finite poset. The *Möbius function* on $\mathcal{P}$, denoted by $\mu_{\mathcal{P}}$, is defined by the following criteria: for any $x, z\in\mathcal{P}$,

$$\begin{aligned}
\mu_{\mathcal{P}}(x,z)&=0 &&\text{if } x\not\leq z,\\
\mu_{\mathcal{P}}(x,z)&=1 &&\text{if } x=z,\\
\textstyle\sum_{x\leq y\leq z}\mu_{\mathcal{P}}(x,y)&=0 &&\text{if } x<z.
\end{aligned}$$

A classic reference for Möbius functions is [Rota 1964]. In this section, we need to study a variant of the Möbius function on the poset of subgroups of a finite group (ordered by inclusion). For a history of the work on the Möbius function on this poset, see [Hawkes et al. 1989]. Now, for any finite group G, let $\mathcal{P}_G$ be the poset of subgroups of G ordered by inclusion. For $A\in\mathcal{G}$, we study an amalgam of the Möbius functions on $\mathcal{P}_A$ and $\mathcal{G}$, which we define below.

Notation 4.1.1. For any $A, B\in\mathcal{G}$, let $\mathrm{sub}(A,B)$ be the number of subgroups of B that are isomorphic to A. If $A\in\mathcal{G}$, an *A-chain* is a finite (possibly empty) linearly ordered subset of $\{B\in\mathcal{G}\mid B>A\}$. Now, given an A-chain $\mathfrak{C}=\{A_j\}_{j=1}^{i}$, with $A_j<A_{j+1}$ for all $j\in\{1,\dots,i-1\}$, define

$$\mathrm{sub}(\mathfrak{C}):=(-1)^i\,\mathrm{sub}(A,A_1)\prod_{j=1}^{i-1}\mathrm{sub}(A_j,A_{j+1}).$$

(We set $\mathrm{sub}(\mathfrak{C}) = 1$ if $\mathfrak{C}$ is empty.) Finally, for any $A, B \in \mathcal{G}$, let

$$S(A, B) = \begin{cases} 0 & \text{if } A \not\leq B, \\ 1 & \text{if } A = B, \\ \displaystyle\sum_{\substack{A\text{-chains } \mathfrak{C}, \\ \max \mathfrak{C} = B}} \mathrm{sub}(\mathfrak{C}) & \text{if } A < B. \end{cases}$$

Remark 4.1.2. Though S is defined on the poset $\mathcal{G}$, it is closely related to the classical work on the Möbius function on the subgroup lattice of a fixed group. Indeed, by applying Lemma 2.2 of [Hawkes et al. 1989], we see that if $A, B \in \mathcal{G}$, then

$$S(A, B) = \sum_{\substack{C \leq B \\ C \simeq A}} \mu_B(C, B).$$

Given $x \in (\mathbb{Z}_\ell)^\times$, we can use the function S defined in Notation 4.1.1 to begin our analysis of the measure μ_x, following the outline in Goal 2.2.3.

Lemma 4.1.3. *Suppose $A \in \mathcal{G}$, $g, \rho \in \mathbb{Z}^{>0}$ and $\xi \in \mathbb{Z}^{\geq 0}$, with $\rho \geq \xi$ and $\ell^\rho \geq \exp A$. Then*

$$o_{2g,\rho}^{A,\langle\xi\rangle} \, |\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)| = \sum_{\substack{B \in \mathcal{G} \\ B \leq (R_\rho)^{2g}}} N_{2g,\rho}^{\langle\xi\rangle}(B) \, |\mathrm{Inj}(A, B)|.$$

Proof. Applying Lemma 3.2.6 and Burnside's counting theorem, we see that

$$\begin{aligned} o_{2g,\rho}^{A,\langle\xi\rangle} |\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)| &= \sum_{\gamma \in \mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)} |\mathrm{Fix}(\gamma)| = \sum_{\gamma \in \mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)} |\mathrm{Inj}(A, \ker(\mathrm{Id} - \gamma))| \\ &= \sum_{\substack{B \in \mathcal{G} \\ B \leq (R_\rho)^{2g}}} N_{2g,\rho}^{\langle\xi\rangle}(B) \, |\mathrm{Inj}(A, B)|, \end{aligned}$$

where the last step follows from Lemma 3.1.4. □

For A, g, ρ, ξ as above, Lemma 4.1.3 gives us an "upper triangular" system of equations, which we will solve for $N_{2g,\rho}^{\langle\xi\rangle}(A)$. (The quotes indicate that the system is indexed by the poset $\mathcal{P}_{(R_\rho)^{2g}}$.) Proposition 4.1.4 is the first step along this path.

Proposition 4.1.4. *Suppose A, g, ρ, ξ are as above. Then*

$$\frac{N_{2g,\rho}^{\langle\xi\rangle}(A)}{|\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)|} = \sum_{\substack{B \in \mathcal{G} \\ B \leq (R_\rho)^{2g}}} o_{2g,\rho}^{B,\langle\xi\rangle} \cdot \frac{S(A, B)}{|\mathrm{Aut}\, B|}.$$

Proof. We use strong induction on $|(R_\rho)^{2g}|/|A|$. In light of Lemma 4.1.3, the base case $A = (R_\rho)^{2g}$ is trivial. Now suppose the result is true for all $B \in \mathcal{G}$ with

$B \le (R_\rho)^{2g}$ and $|(R_\rho)^{2g}|/|B| < |(R_\rho)^{2g}|/|A|$. Using Lemma 4.1.3, we see that

$$\begin{aligned}\frac{N^{\langle\xi\rangle}_{2g,\rho}(A)}{|\mathrm{GSp}^{\langle\xi\rangle}_{2g}(R_\rho)|} &= \frac{1}{|\mathrm{Aut}\,A|}\cdot\Biggl(o^{A,\langle\xi\rangle}_{2g,\rho} - \frac{1}{|\mathrm{GSp}^{\langle\xi\rangle}_{2g}(R_\rho)|}\cdot\sum_{\substack{B\in\mathcal{G}\\ B\le(R_\rho)^{2g}\\ B\ne A}} N^{\langle\xi\rangle}_{2g,\rho}(B)\,|\mathrm{Inj}(A,B)|\Biggr)\\ &= \frac{o^{A,\langle\xi\rangle}_{2g,\rho}}{|\mathrm{Aut}\,A|} - \sum_{\substack{B\in\mathcal{G}\\ B\le(R_\rho)^{2g}\\ B\ne A}} \frac{N^{\langle\xi\rangle}_{2g,\rho}(B)}{|\mathrm{GSp}^{\langle\xi\rangle}_{2g}(R_\rho)|}\cdot\mathrm{sub}(A,B),\end{aligned}$$

so the result follows by the induction hypothesis. □

4.2. ***Vanishing of the Möbius function.*** Before proceeding, we need a bit more notation, and two results from [Garton 2014b].

Notation 4.2.1. For any $A\in\mathcal{G}$ and any $i\in\mathbb{Z}^{\ge 0}$, let

$$A_{\oplus i} := A\oplus\overbrace{(\mathbb{Z}/\ell)\oplus\cdots\oplus(\mathbb{Z}/\ell)}^{i\text{ times}}.$$

Hall [1934] proved that if G is an ℓ-group of order ℓ^n, then $\mu_G(1,G)=0$ unless G is elementary abelian, in which case $\mu_G(1,G)=(-1)^n\ell^{\binom{n}{2}}$. There is an analogous result for the function S:

Theorem 4.2.2 [Garton 2014b]. *If $A, B\in\mathcal{G}$, then $S(A,B)=0$ unless there exists an injection $\iota : A\hookrightarrow B$ with* coker(ι) *elementary abelian.*

Additionally, this property of S will prove helpful:

Theorem 4.2.3 [ibid.]. *If $A, B\in\mathcal{G}$ and $B=C_{\oplus i}$ for some $C\in\mathcal{G}$ with* $\mathrm{rank}\,C = \mathrm{rank}\,A$ *and $i\in\mathbb{Z}^{\ge 0}$, then $S(A,B)=S(A,C)\cdot S(C,B)$.*

Theorem 4.2.2 and Theorem 4.2.3 have the following corollary:

Corollary 4.2.4. *Suppose A, g, ρ, ξ are as above, and let $r=\mathrm{rank}\,A$. If in addition we know $\xi\in\mathbb{Z}^{>0}$ and ρ satisfies $\rho>\xi$ and $\ell^\rho>\exp A$, then*

$$\nu^{\langle\xi\rangle}_{2g,\rho}(A) = \sum_{B\in\mathcal{G}(r)} S(A,B)\cdot\sum_{i=0}^{2g-r}\frac{\ell o^{B_{\oplus i},\langle\xi\rangle}_{2g,\rho} - o^{B_{\oplus i},\langle\xi+1\rangle}_{2g,\rho}}{\ell-1}\cdot\frac{S(B,B_{\oplus i})}{|\mathrm{Aut}\,B_{\oplus i}|}.$$

Proof. Using the fact that $|\mathrm{GSp}^{\langle\xi\rangle}_{2g}(R_\rho)| = \ell\,|\mathrm{GSp}^{\langle\xi+1\rangle}_{2g}(R_\rho)|$, note that

$$\begin{aligned}\nu^{\langle\xi\rangle}_{2g,\rho}(A) &= \frac{N^{\langle\xi\rangle}_{2g,\rho}(A) - N^{\langle\xi+1\rangle}_{2g,\rho}(A)}{|\mathrm{GSp}^{\langle\xi\rangle}_{2g}(R_\rho)| - |\mathrm{GSp}^{\langle\xi+1\rangle}_{2g}(R_\rho)|}\\ &= \frac{\ell N^{\langle\xi\rangle}_{2g,\rho}(A)}{(\ell-1)\,|\mathrm{GSp}^{\langle\xi\rangle}_{2g}(R_\rho)|} - \frac{N^{\langle\xi+1\rangle}_{2g,\rho}(A)}{(\ell-1)\,|\mathrm{GSp}^{\langle\xi+1\rangle}_{2g}(R_\rho)|}.\end{aligned}$$

Applying Proposition 4.1.4, we obtain

$$\nu_{2g,\rho}^{\langle\xi\rangle}(A)=\sum_{\substack{B\in\mathcal{G}\\ B\leq(R_\rho)^{2g}}}\frac{\ell o_{2g,\rho}^{B,\langle\xi\rangle}-o_{2g,\rho}^{B,\langle\xi+1\rangle}}{\ell-1}\cdot\frac{S(A,B)}{|\operatorname{Aut}B|}.$$

Now, by Theorem 4.2.2 we know that if $B\in\mathcal{G}$ is not of the form $B=C_{\oplus i}$ for some $C\in\mathcal{G}(r)$ and some $i\in\mathbb{Z}^{\geq 0}$, then $S(A,B)$ vanishes. Thus, by Theorem 4.2.3, we conclude that

$$\nu_{2g,\rho}^{\langle\xi\rangle}(A)=\sum_{B\in\mathcal{G}(r)}S(A,B)\cdot\sum_{i=0}^{2g-r}\frac{\ell o_{2g,\rho}^{B_{\oplus i},\langle\xi\rangle}-o_{2g,\rho}^{B_{\oplus i},\langle\xi+1\rangle}}{\ell-1}\cdot\frac{S(B,B_{\oplus i})}{|\operatorname{Aut}B_{\oplus i}|},$$

as desired. □

Note 4.2.5. Suppose A, g, ρ, ξ, r are as in Corollary 4.2.4, and suppose that $g\geq r$. Then for any $B\in\mathcal{G}(r)$ and $i\in\{0\ldots,g-r\}$, we know by Note 3.2.5 and Note 3.2.2 that

$$\frac{\ell o_{2g,\rho}^{B_{\oplus i},\langle\xi\rangle}-o_{2g,\rho}^{B_{\oplus i},\langle\xi+1\rangle}}{\ell-1}=|\Lambda(B_{\oplus i}/\ell^{\xi})|=\ell^{ir+\frac{i(i-1)}{2}}|\Lambda(B/\ell^{\xi}B)|,$$

and for any $i\in\{g-r+1,\ldots,2g-r\}$, we can use the proof of Lemma 3.2.3 to note that

$$\frac{\ell o_{2g,\rho}^{B_{\oplus i},\langle\xi\rangle}-o_{2g,\rho}^{B_{\oplus i},\langle\xi+1\rangle}}{\ell-1}\leq\ell o_{2g,\rho}^{B_{\oplus i},\langle\xi\rangle}\leq\ell|\Lambda(B_{\oplus i})|=\ell^{ir+\frac{i(i-1)}{2}+1}|\Lambda(B)|.$$

Thus, if

$$\sum_{i=0}^{\infty}\ell^{ir+\frac{i(i-1)}{2}}\frac{S(B,B_{\oplus i})}{|\operatorname{Aut}B_{\oplus i}|}$$

converges absolutely (and it does; see Lemmas 5.1.2 and 5.1.3 and Theorem 5.1.4), then so does

$$\sum_{i=0}^{\infty}\frac{\ell o_{2g,\rho}^{B_{\oplus i},\langle\xi\rangle}-o_{2g,\rho}^{B_{\oplus i},\langle\xi+1\rangle}}{\ell-1}\cdot\frac{S(B,B_{\oplus i})}{|\operatorname{Aut}B_{\oplus i}|},$$

and

$$\lim_{g\to\infty}\nu_{2g,\rho}^{\langle\xi\rangle}(A)=\sum_{B\in\mathcal{G}(r)}S(A,B)|\Lambda(B/\ell^{\xi}B)|\cdot\sum_{i=0}^{\infty}\ell^{ir+\frac{i(i-1)}{2}}\frac{S(B,B_{\oplus i})}{|\operatorname{Aut}B_{\oplus i}|}.$$

Analyzing the inner series is the subject of the next section. (Note that this limit does not depend on ρ, once ρ is large enough; this is consistent with Lemma 2.2.1.)

5. q-series and convergence

5.1. ***q*-series.** Before continuing, we make a small foray into some q-series notation and calculations.

Notation 5.1.1. For $z, q \in \mathbb{C}$ with $|q| < 1$ and $i \in \mathbb{Z}^{\geq 0}$, let

$$(z;q)_i := \prod_{j=0}^{i-1} (1 - q^j z).$$

To ease notation, set $(q)_i := (q;q)_i$. Recall the definition of the q-binomial coefficients: for any $k, m \in \mathbb{Z}^{\geq 0}$, let

$$\binom{k}{m}_q := \frac{(q)_k}{(q)_m (q)_{k-m}},$$

with $\binom{k}{m}_q := 0$ if $k < m$.

For $i \in \mathbb{Z}^{\geq 0}$, let $r_i = -1/(\ell^{\frac{i(i+1)}{2}}(\ell^{-1})_i)$. We define the next object in terms of any finite set of nonnegative integers S and any $i \in \mathbb{Z}$ satisfying $i > \max S$. If $S \cup \{0\} = \{s_0, \ldots, s_j\}$, where $0 = s_0 < s_1 < \cdots < s_{j+1} := i$, define $r_S^i = \prod_{i=0}^{j} r_{s_{i+1}-s_i}$.

Finally, let $t_0 = 1$, let $t_1 = r_\varnothing^1$, and for $i > 1$, let

$$t_i = \sum_{S \subseteq \{1, \ldots i-1\}} r_S^i.$$

Lemma 5.1.2.
$$\sum_{i=0}^{\infty} t_i = \prod_{i=1}^{\infty} (1 + \ell^{-i})^{-1}.$$

Proof. Let $R = r_1 + r_2 + \cdots$ and, to get into the spirit of a q-series calculation, let $q = \ell^{-1}$. Using a product formula of Euler (see [Andrews 1976, p. 19]), we note that

$$R = -\sum_{i=1}^{\infty} \frac{q^{\frac{i(i+1)}{2}}}{(1-q^i)\cdots(1-q)} = -\sum_{i=1}^{\infty} \frac{q^i q^{\frac{i(i-1)}{2}}}{(1-q^i)\cdots(1-q)} = 1 - \prod_{i=1}^{\infty} (1+q^i).$$

Now, by the definition of t_i (and by using Lemma 5.1.3 to rearrange the terms of the sum), we know

$$\sum_{i=0}^{\infty} t_i = 1 + R + R^2 + R^3 + \cdots = \frac{1}{1-R} = \prod_{i=1}^{\infty} (1 + \ell^{-i})^{-1},$$

as desired. □

Next, we justify the reordering of the summands in Lemma 5.1.2:

Lemma 5.1.3. *For any finite set of nonnegative integers S and $i \in \mathbb{Z}$ satisfying $i > \max S$, let $\rho_S^i := |r_S^i|$. Next, let $\tau_0 = 1$, let $\tau_1 = \rho_\varnothing^1$, and for any $i > 1$, let*

$$\tau_i := \sum_{S \subseteq \{1,\dots i-1\}} \rho_S^i.$$

Then $\sum_{i=0}^\infty \tau_i$ converges.

Proof. For fun, we will give two proofs: a simple proof that holds for any $\ell > 3$, and a more complicated one that holds for $\ell \geq 3$. Note that the sum clearly diverges for $\ell = 2$ since it includes infinitely many 1s.

For the simple proof, note that for any finite set S of nonnegative integers and any $i > \max S$, we know $\rho_S^i \leq (\ell-1)^{-i}$. It follows that for any $i \in \mathbb{Z}^{\geq 0}$, we have that $\tau_i \leq 2^{i-1}(\ell-1)^{-i}$, so $\sum_{i=0}^\infty \tau_i$ converges for $\ell > 3$.

Of course, this argument fails for $\ell = 3$. In this case, for a finite set S of nonnegative integers and an $i > \max S$, we must use a (slightly) better bound than $\rho_S^i \leq (\ell-1)^{-i}$. Let $\lambda = (\ell-1)^{-1}$. Since $(\ell^m-1)^{-1} \leq (\ell-1)^{-m}$ for any $m \in \mathbb{Z}^{\geq 0}$, if we let $S \cup \{0\} = \{s_0, \dots, s_j\}$, where $0 = s_0 < s_1 < \cdots < s_{j+1} := i$, then

$$\rho_S^i = \prod_{k=0}^{j} |r_{s_{k+1}-s_k}| \leq \prod_{k=0}^{j} \lambda^{\frac{1}{2}(s_{k+1}-s_k)(s_{k+1}-s_k+1)}. \tag{1}$$

Let T_i be the number of compositions of i by triangular numbers. By rearranging the terms of $\sum_{i=0}^\infty \tau_i$ to order them by the exponent of λ appearing in the bound (1), we see that if $\sum_{i=1}^\infty T_i\lambda^i$ converges, then so does $\sum_{i=0}^\infty \tau_i$. Since the generating function for the number of compositions of positive triangular numbers is

$$\sum_{i=0}^\infty T_i x^i = \frac{1}{1-\sum_{j=1}^\infty x^{\frac{1}{2}j(j+1)}}, \tag{2}$$

we need only show that the radius of convergence of (2) is at least λ. Since $\ell \geq 3$, we know that $\lambda \leq \frac{1}{2}$, and

$$1 > \tfrac{1}{2} + (\tfrac{1}{2})^3 + (\tfrac{1}{2})^6 + (\tfrac{1}{2})^{10} + \cdots,$$

so the lemma is true. □

We can now finish proving the result mentioned in Note 4.2.5.

Theorem 5.1.4. *Suppose $A \in \mathscr{G}$, $\rho, \xi \in \mathbb{Z}^{>0}$, and let $r = \operatorname{rank} A$. If $\rho > \xi$ and $\ell^\rho > \exp A$, then*

$$\lim_{g\to\infty} \nu_{2g,\rho}^{\langle\xi\rangle}(A) = \prod_{i=1}^\infty (1+\ell^{-i})^{-1} \cdot \sum_{B \in \mathscr{G}(r)} |\Lambda(B/\ell^\xi B)| \cdot \frac{S(A,B)}{|\operatorname{Aut} B|}.$$

Proof. Let $B \in \mathscr{G}(r, s)$, let S be a finite set of nonnegative integers, and let i be a positive integer with $i > \max S$. Suppose $S \cup \{0\} = \{s_0, \dots, s_j\}$, where $0 = s_0 < \cdots < s_{j+1} := i$. Now, we know by [Garton 2014a] that, for any $k, m \in \mathbb{Z}^{\geq 0}$ with $k \leq m$,

$$\operatorname{sub}(B_{\oplus k}, B_{\oplus m}) = \frac{\ell^{(r+k)(m-k)}(\ell^{-1})_{r-s+m}}{(\ell^{-1})_{r-s+i}(\ell^{-1})_{m-k}}$$

and

$$|\operatorname{Aut} B_{\oplus i}| = \frac{\ell^{2ir+i^2}(\ell^{-1})_{r-s+i}}{(\ell^{-1})_{r-s}}|\operatorname{Aut} B|,$$

so

$$\begin{aligned}
&(-1)^{j+1} \cdot \frac{\ell^{ir+\frac{i(i-1)}{2}}}{|\operatorname{Aut} B_{\oplus i}|} \cdot \prod_{k=0}^{j} \operatorname{sub}(B_{\oplus s_k}, B_{\oplus s_{k+1}}) \\
&= (-1)^{j+1} \cdot \frac{\ell^{-ir-\frac{i(i+1)}{2}}}{|\operatorname{Aut} B|} \cdot \frac{(\ell^{-1})_{r-s}}{(\ell^{-1})_{r-s+i}} \cdot \prod_{k=0}^{j} \frac{\ell^{(r+s_k)(s_{k+1}-s_k)}(\ell^{-1})_{r-s+s_{k+1}}}{(\ell^{-1})_{r-s+s_k}(\ell^{-1})_{s_{k+1}-s_k}} \\
&= (-1)^{j+1} \cdot \frac{\ell^{-ir-\frac{i(i+1)}{2}}}{|\operatorname{Aut} B|} \cdot \prod_{k=0}^{j} \frac{\ell^{(r+s_k)(s_{k+1}-s_k)}}{(\ell^{-1})_{s_{k+1}-s_k}} \\
&= (-1)^{j+1} \cdot \frac{1}{|\operatorname{Aut} B|} \cdot \prod_{k=0}^{j} \frac{\ell^{-\frac{1}{2}(s_{k+1}-s_k)(s_{k+1}-s_k+1)}}{(\ell^{-1})_{s_{k+1}-s_k}}.
\end{aligned}$$

But by Lemma 5.1.2, this means that

$$\sum_{i=0}^{\infty} \ell^{ir+\frac{i(i-1)}{2}} \frac{S(B, B_{\oplus i})}{|\operatorname{Aut} B_{\oplus i}|} = \frac{1}{|\operatorname{Aut} B|} \cdot \sum_{i=0}^{\infty} t_i = \frac{1}{|\operatorname{Aut} B|} \cdot \prod_{i=1}^{\infty} (1 + \ell^{-i})^{-1},$$

so we conclude by Note 4.2.5. □

5.2. *The main results.* To conclude we mention two corollaries of Theorem 5.1.4, one trivial and one nontrivial.

Corollary 5.2.1. *If* $x \in (\mathbb{Z}_\ell)^\times$ *satisfies* $x \equiv 1 \pmod{\ell}$, *then*

$$\lim_{g \to \infty} \mu_{2g}^{(x)}(\{0\}) = \prod_{i=1}^{\infty} (1 + \ell^{-i})^{-1}.$$

Friedman and Washington [1989] proved the analog of Corollary 5.2.1 for the groups $\mathrm{GL}_n(\mathbb{Z}_\ell)$; namely, they proved that

$$\lim_{g \to \infty} \mu_{\mathrm{GL}_n(\mathbb{Z}_\ell)}(\{\phi \in \mathrm{GL}_n(\mathbb{Z}_\ell) \mid \operatorname{coker}(\mathrm{Id} - \phi) \simeq \{0\}\}) = \prod_{i=1}^{\infty} (1 - \ell^{-i}),$$

where $\mu_{\mathrm{GL}_n(\mathbb{Z}_\ell)}$ is the normalized Haar measure on $\mathrm{GL}_n(\mathbb{Z}_\ell)$. Friedman and Washington expressed the hope that the statistics of $\mathrm{GL}_n(\mathbb{Z}_\ell)$ (as $n \to \infty$) would match those of $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ (as $2g \to \infty$). Achter [2006] proved that this was not the case. Corollary 5.2.1 calculates a particular statistic for $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ (as $2g \to \infty$). It is noteworthy that the quantity in Corollary 5.2.1 matches Malle's conjectured probability that the class numbers of relative class groups are coprime to ℓ (when the base field of the extension has ℓth roots of unity but not ℓ^2th roots of unity; see Conjecture 2.1 in [Malle 2010]). Furthermore, Corollary 5.2.2 shows that the distribution on $\mathcal{G}$ proposed by Malle matches the distribution on $\mathcal{G}$ given by $\mu_{2g}^{(x)}$ for any $x \in (\mathbb{Z}_\ell)^\times$ with $x \equiv 1 \pmod{\ell}$ but $x \not\equiv 1 \pmod{\ell^2}$. Moreover, Corollary 5.2.2 also computes the distribution on $\mathcal{G}$ given by $\mu_{2g}^{(x)}$ when $x \equiv 2 \pmod{\ell}$ but $x \not\equiv 1 \pmod{\ell^3}$; this is analogous to the number field case when the base field has ℓ^2th roots of unity but not ℓ^3th roots of unity. The proof of Corollary 5.2.2 relies heavily on calculations from [Garton 2014a].

Corollary 5.2.2. *Suppose $r, s \in \mathbb{Z}^{\geq 0}$ with $r \geq s$. Furthermore, suppose that $x \in \mathbb{Z}_\ell$ and $\xi \in \mathbb{Z}^{>0}$ with $x \equiv 1 \pmod{\ell^\xi}$ but $x \not\equiv 1 \pmod{\ell^{\xi+1}}$. If $A \in \mathcal{G}(r, s)$, then*

$$\lim_{g\to\infty} \mu_{2g}^{(x)}(A) = \begin{cases} \ell^{\frac{r(r-1)}{2}} \cdot (\ell^{-1})_r \cdot \dfrac{\prod_{i=1}^{\infty}(1+\ell^{-i})^{-1}}{|\mathrm{Aut}\, A|} & \text{if } \xi = 1, \\ \ell^{\frac{r(r-1)}{2}+\frac{s(s-1)}{2}} \cdot (\ell^{-1})_s (\ell^{-1}; \ell^{-2})_{\lceil \frac{r-s}{2} \rceil} \cdot \dfrac{\prod_{i=1}^{\infty}(1+\ell^{-i})^{-1}}{|\mathrm{Aut}\, A|} & \text{if } \xi = 2. \end{cases}$$

Proof. Choose any $\rho \in \mathbb{Z}^{>0}$ with $\rho > \xi$ and $\ell^\rho > \exp A$. Then by Lemma 2.2.1 we know

$$\mu_{2g}^{(x)}(A) = \nu_{2g,\rho}^{\langle \xi \rangle}(A).$$

Now, we know from [Garton 2014a] that

$$\sum_{B \in \mathcal{G}(r)} \frac{S(A, B)}{|\mathrm{Aut}\, B|} = \frac{(\ell^{-1})_r}{|\mathrm{Aut}\, A|},$$

and, for any $i \in \{s, \ldots, r\}$,

$$\sum_{B \in \mathcal{G}(r,i)} \frac{S(A, B)}{|\mathrm{Aut}\, B|} = (-1)^{i-s} \cdot \ell^{\frac{s(s+1)}{2} - \frac{i(i+1)}{2}} \cdot \binom{r-s}{r-i}_{\ell^{-1}} \cdot \frac{(\ell^{-1})_s}{|\mathrm{Aut}\, A|}.$$

The $\xi = 1$ case follows from Note 3.2.2. For $\xi = 2$, use Note 3.2.2 again to see that

$$\begin{aligned}\sum_{B\in\mathcal{G}(r)} |\Lambda(B/\ell^2B)|\cdot\frac{S(A,B)}{|\mathrm{Aut}\,B|} &= \sum_{i=s}^{r}\sum_{B\in\mathcal{G}(r,i)} |\Lambda(B/\ell^2B)|\cdot\frac{S(A,B)}{|\mathrm{Aut}\,B|}\\ &= \sum_{i=s}^{r}(-1)^{i-s}\cdot\ell^{\frac{r(r-1)}{2}+\frac{s(s+1)}{2}-i}\cdot\binom{r-s}{r-i}_{\ell^{-1}}\cdot\frac{(\ell^{-1})_s}{|\mathrm{Aut}\,A|}\\ &= \frac{\ell^{\frac{r(r-1)}{2}+\frac{s(s+1)}{2}}(\ell^{-1})_s}{|\mathrm{Aut}\,A|}\cdot\sum_{i=s}^{r}(-1)^{i-s}\cdot\binom{r-s}{r-i}_{\ell^{-1}}\cdot\ell^{-i}.\end{aligned}$$

Letting $k=r-s$ and $q=1/\ell$, we apply formula (1.10) from [Kupershmidt 2000], which is a corollary of formula (1.12), to obtain

$$\begin{aligned}\sum_{B\in\mathcal{G}(r)} |\Lambda(B/\ell^2B)|\cdot\frac{S(A,B)}{|\mathrm{Aut}\,B|} &= \frac{\ell^{\frac{r(r-1)}{2}+\frac{s(s-1)}{2}}(\ell^{-1})_s}{|\mathrm{Aut}\,A|}\cdot\sum_{i=0}^{k}(-1)^i\binom{k}{i}_q q^i\\ &= \frac{\ell^{\frac{r(r-1)}{2}+\frac{s(s-1)}{2}}(\ell^{-1})_s}{|\mathrm{Aut}\,A|}\cdot(q;q^2)_{\lceil\frac{k}{2}\rceil},\end{aligned}$$

as desired. □

References

[Achter 2006] J. D. Achter, "The distribution of class groups of function fields", *J. Pure Appl. Algebra* **204**:2 (2006), 316–333. MR 2006h:11132 Zbl 1134.11042

[Achter 2008] J. D. Achter, "Results of Cohen–Lenstra type for quadratic function fields", pp. 1–7 in *Computational arithmetic geometry* (San Francisco, 2006), edited by K. E. Lauter and K. A. Ribet, Contemp. Math. **463**, Amer. Math. Soc., Providence, RI, 2008. MR 2009j:11101 Zbl 1166.11018

[Adam 2014a] M. Adam, "On the distribution of eigenspaces in classical groups over finite rings", *Linear Algebra Appl.* **443** (2014), 50–65. MR 3148893 Zbl 1292.20076

[Adam 2014b] M. Adam, *On the distribution of eigenspaces in classical groups over finite rings and the Cohen–Lenstra heuristic*, Ph.D. thesis, Technischen Universität Kaiserslautern, 2014, https://kluedo.ub.uni-kl.de/files/3732/Diss_Adam86.pdf.

[Adam and Malle 2015] M. Adam and G. Malle, "A class group heuristic based on the distribution of 1-eigenspaces in matrix groups", *J. Number Theory* **149** (2015), 225–235. MR 3296009

[Andrews 1976] G. E. Andrews, *The theory of partitions*, Encyclopedia of Mathematics and its Applications **2**, Addison-Wesley, Reading, MA, 1976. MR 58 #27738

[Cohen and Lenstra 1984] H. Cohen and H. W. Lenstra, Jr., "Heuristics on class groups of number fields", pp. 33–62 in *Number theory* (Noordwijkerhout, Netherlands, 1983), edited by H. Jager, Lecture Notes in Math. **1068**, Springer, Berlin, 1984. MR 85j:11144 Zbl 0558.12002

[Cohen and Martinet 1990] H. Cohen and J. Martinet, "Étude heuristique des groupes de classes des corps de nombres", *J. Reine Angew. Math.* **404** (1990), 39–76. MR 91k:11097 Zbl 0699.12016

[Ellenberg et al. 2009] J. S. Ellenberg, A. Venkatesh, and C. Westerland, "Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields", preprint, 2009. arXiv 0912.0325

[Friedman and Washington 1989] E. Friedman and L. C. Washington, "On the distribution of divisor class groups of curves over a finite field", pp. 227–239 in *Théorie des nombres* (Université Laval, Quebec City, 1987), edited by J.-M. De Koninck and C. Levesque, de Gruyter, Berlin, 1989. MR 91e:11138 Zbl 0693.12013

[Garton 2012] D. Garton, *Random matrices and Cohen–Lenstra statistics for global fields with roots of unity*, Ph.D. thesis, University of Wisconsin, Madison, 2012, http://search.proquest.com/docview/1039288336.

[Garton 2014a] D. Garton, "Some finite abelian group theory and some q-series identities", preprint, 2014. To appear in *Ann. Comb.* arXiv 1405.5824

[Garton 2014b] D. Garton, "A weighted Möbius function", preprint, 2014. arXiv 1405.5818

[Hall 1934] P. Hall, "A Contribution to the Theory of Groups of Prime-Power Order", *Proc. London Math. Soc.* **S2-36**:1 (1934), 29–95. MR 1575964 Zbl 59.0147.02

[Hall 1938] P. Hall, "A partition formula connected with Abelian groups", *Comment. Math. Helv.* **11**:1 (1938), 126–129. MR 1509594 Zbl 0019.39705

[Hawkes et al. 1989] T. Hawkes, I. M. Isaacs, and M. Özaydin, "On the Möbius function of a finite group", *Rocky Mountain J. Math.* **19**:4 (1989), 1003–1034. MR 90k:20046 Zbl 0708.20005

[Katz and Sarnak 1999] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications **45**, American Mathematical Society, Providence, RI, 1999. MR 2000b:11070 Zbl 0958.11004

[Kupershmidt 2000] B. A. Kupershmidt, "q-Newton binomial: from Euler to Gauss", *J. Nonlinear Math. Phys.* **7**:2 (2000), 244–262. MR 2002e:33024 Zbl 0955.33012

[Malle 2008] G. Malle, "Cohen–Lenstra heuristic and roots of unity", *J. Number Theory* **128**:10 (2008), 2823–2835. MR 2009j:11179 Zbl 1225.11143

[Malle 2010] G. Malle, "On the distribution of class groups of number fields", *Experiment. Math.* **19**:4 (2010), 465–474. MR 2011m:11224 Zbl 1297.11139

[Matchett Wood 2014] M. Matchett Wood, "The distribution of sandpile groups of random graphs", preprint, 2014. arXiv 1402.5149

[McDonald 1976] B. R. McDonald, *Geometric algebra over local rings*, Pure and Applied Mathematics **36**, Marcel Dekker, New York, 1976. MR 57 #16198 Zbl 0346.20027

[Michael 2006] A. A. G. Michael, "Finite abelian actions on surfaces", *Topology Appl.* **153**:14 (2006), 2591–2612. MR 2007c:57026 Zbl 1103.57023

[Rota 1964] G.-C. Rota, "On the foundations of combinatorial theory, I: Theory of Möbius functions", *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* **2** (1964), 340–368. MR 30 #4688 Zbl 0121.02406

Communicated by Bjorn Poonen
Received 2014-05-26 Revised 2014-11-18 Accepted 2014-12-25

gartondw@pdx.edu *Fariborz Maseeh Department of Mathematics and Statistics,*
Portland State University, PO Box 751,
Portland, OR 97207-0751, United States

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2015 is US $255/year for the electronic version, and $440/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 9 No. 1 2015

1937-0652(2015)9:1;1-8