Random Dieudonné modules, random \$p\$-divisible groups, and random curves over finite fields

Bryden Cais, Jordan S. Ellenberg and David Zureick-Brown

Journal of the Institute of Mathematics of Jussieu / Volume 12 / Issue 03 / July 2013, pp 651 - 676
DOI: 10.1017/S1474748012000862, Published online: 13 February 2013

J. Inst. Math. Jussieu (2013) **12**(3), 651–676
doi:10.1017/S1474748012000862

RANDOM DIEUDONNÉ MODULES, RANDOM p-DIVISIBLE GROUPS, AND RANDOM CURVES OVER FINITE FIELDS

BRYDEN CAIS[1], JORDAN S. ELLENBERG[2] AND DAVID ZUREICK-BROWN[3]

[1] *Department of Mathematics, The University of Arizona, 617 N. Santa Rita Ave., P.O. Box 210089, Tucson, AZ 85721-0089, USA* (cais@math.arizona.edu)
[2] *Department of Mathematics, University of Wisconsin-Madison, 480 Lincoln Drive, Madison, WI 53706, USA* (ellenber@math.wisc.edu)
[3] *Dept. of Math and Computer Science, Emory University, 400 Dowman Dr., W401, Atlanta, GA 30322, USA* (dzb@mathcs.emory.edu)

(Received 12 September 2012; revised 22 November 2012; accepted 23 November 2012; first published online 13 February 2013)

Abstract We describe a probability distribution on isomorphism classes of principally quasi-polarized p-divisible groups over a finite field k of characteristic p which can reasonably be thought of as a 'uniform distribution', and we compute the distribution of various statistics (p-corank, a-number, etc.) of p-divisible groups drawn from this distribution. It is then natural to ask to what extent the p-divisible groups attached to a randomly chosen hyperelliptic curve (respectively, curve; respectively, abelian variety) over k are uniformly distributed in this sense. This heuristic is analogous to conjectures of Cohen–Lenstra type for char $k \neq p$, in which case the random p-divisible group is defined by a random matrix recording the action of Frobenius. Extensive numerical investigation reveals some cases of agreement with the heuristic and some interesting discrepancies. For example, plane curves over $\mathbf{F}_3$ appear substantially less likely to be ordinary than hyperelliptic curves over $\mathbf{F}_3$.

Keywords: algebraic curve; arithmetic statistics; p-divisible group; Dieduonne module; random matrices

AMS 2010 *Mathematics subject classification:* 14L05; 11G20; 14G17

1. Introduction

Let q be a power of a prime p, and let $C/\mathbf{F}_q$ be a genus-g hyperelliptic curve with affine equation

$$y^2 = f(x),$$

where f is chosen *at random* from the set of monic squarefree polynomials of degree $2g+1$. We can think of $\mathbf{F}_q(C)$ as a 'random quadratic extension of $\mathbf{F}_q(t)$', and ask about the probability distribution (if there is one) on arithmetic invariants of C.

For example: if ℓ is an odd prime not equal to p, one can ask about the distribution of the ℓ-primary part of the ideal class group $\mathrm{Cl}(\mathbf{F}_q(C))$, or, equivalently, the group of

The first and third authors are supported by NSA Young Investigator grants. The second author is supported by an NSF grant and a Romnes Family Fellowship.

$\mathbf{F}_q$-rational points of the ℓ-divisible group $J(C)[\ell^\infty]$. The distribution of $\mathrm{Cl}(\mathbf{F}_q(C))[\ell^\infty]$ is the subject of the *Cohen–Lenstra conjectures* [6], which predict that the probability distribution on the isomorphism classes of $\mathrm{Cl}(\mathbf{F}_q(C))[\ell^\infty]$ approaches a limit, the so-called *Cohen–Lenstra distribution*, as $g \to \infty$. More precisely, Cohen and Lenstra proposed this conjecture for the class groups of quadratic number fields, but it was quickly understood (see, e.g., [12]) that the underlying philosophy was just as valid for hyperelliptic function fields.

Much less effort has been devoted to the case where $\ell = p$, perhaps because this question about function fields has no obvious number field analogue. Nonetheless, it is quite natural to ask whether the p-adic invariants of random hyperelliptic curves over $\mathbf{F}_q$ (or random curves, or random abelian varieties) obey statistical regularities. For example:

What is the probability that a random hyperelliptic curve has ordinary Jacobian?

More precisely, let $P_o(q, d)$ be the proportion of the $q^d - q^{d-1}$ monic squarefree polynomials $f(x)$ over $\mathbf{F}_q$ of degree d such that the curve C_f with equation $y^2 = f(x)$ has ordinary Jacobian. Then we ask: does $\lim_{d\to\infty} P_o(q, d)$ exist, and if so, what is its value? Of course one can ask similar questions about other invariants of the p-divisible group of $\mathrm{Jac}(C_f)$, such as a-number, p-rank, Newton polygon, or final type.

One can interpret the Cohen–Lenstra conjecture as an assertion that the ℓ-divisible group of $\mathrm{Jac}(C_f)$ behaves like a 'random principally polarized ℓ-divisible group over $\mathbf{F}_q$'. (This point of view begins with Friedman and Washington [12] and has subsequently been refined by Achter [1], Malle [16], and Garton [13].) A principally polarized ℓ-divisible group of rank $2g$ over $\mathbf{F}_q$ is the same thing as an abelian group isomorphic to $(\mathbf{Q}_\ell/\mathbf{Z}_\ell)^{2g}$, equipped with a nondegenerate symplectic form ω and an automorphism F satisfying $\omega(Fx, Fy) = q\omega(x, y)$. In other words, F is chosen from a certain coset of $\mathrm{Sp}_{2g}(\mathbf{Z}_\ell)$ in $\mathrm{GSp}_{2g}(\mathbf{Z}_\ell)$. Choosing F at random with respect to Haar measure then specifies a notion of a 'random ℓ-divisible group of rank $2g$ over $\mathbf{F}_q$', which allows us to compute notions like 'the probability that a principally polarized ℓ-divisible group of rank $2g$ over $\mathbf{F}_q$ has no non-trivial $\mathbf{F}_q$-rational point'. Moreover, as g goes to infinity, this probability approaches a limit; when q is not congruent to 1 mod ℓ, the limit is

$$\prod_{i=1}^{\infty}(1 - \ell^{-1}),$$

which is precisely the Cohen–Lenstra prediction for the probability that $\mathrm{Jac}(C_f)[\ell^\infty](\mathbf{F}_q)$ is trivial.

In the same way, one might ask whether the p-divisible group of $\mathrm{Jac}(C_f)$ is in any sense a 'random principally quasi-polarized p-divisible group over k'. The first task is to define this notion. A p-divisible group over $\mathbf{F}_q$ is determined by its **Dieudonné module**, a free $\mathbf{Z}_q := W(\mathbf{F}_q)$-module with some extra 'semilinear algebra' structures. It turns out that there is a natural correspondence between principally quasi-polarized Dieudonné modules of rank $2g$ over $\mathbf{Z}_q$ a certain double coset of $\mathrm{Sp}_{2g}(\mathbf{Z}_q)$ in the group of $\mathbf{Z}_p$-linear transformations of $\mathbf{Z}_q^{2g}$. From this description one obtains a probability measure on

principally quasi-polarized Dieudonné modules, and thus on principally quasi-polarized p-divisible groups over k. In § 3, we study the statistics of several natural invariants of random principally quasi-polarized p-divisible groups, and show that these approach limiting distributions as g goes to infinity. For example, we prove the following.

Proposition 1.1. *The probability that a random principally quasi-polarized p-divisible group of rank $2g$ over $\mathbf{F}_q$ has a-number r approaches*

$$q^{-\binom{r+1}{2}} \prod_{i=1}^{\infty}(1+q^{-i})^{-1} \prod_{i=1}^{r}(1-q^{-i})^{-1}$$

as $g \to \infty$. In particular, the probability that a random principally quasi-polarized p-divisible group of rank $2g$ over $\mathbf{F}_q$ is **ordinary** *approaches*

$$\prod_{i=1}^{\infty}(1+q^{-i})^{-1} = \prod_{j=1}^{\infty}(1-q^{1-2j}) \tag{1}$$

as $g \to \infty$.

We call the infinite product in (1) the **Malle–Garton constant**, since it is the same constant that occurs in the work of the two named authors on conjectures of Cohen–Lenstra type over fields containing a pth root of unity.

We also compute some statistics for the p-rank and the group of $\mathbf{F}_q$-rational points of a random principally quasi-polarized p-divisible group G; for instance, we find that the probability that the p-rank of G is $g-1$ (one smaller than maximum) is

$$q^{-1} \prod_{i=1}^{\infty}(1+q^{-i})^{-1},$$

and the probability that the group of $\mathbf{F}_q$-rational p-torsion points has dimension r (as an $\mathbf{F}_p$-vector space) is exactly the Cohen–Lenstra probability

$$q^{-r^2} \prod_{i=1}^{r}(1-q^{-i})^{-1} \prod_{j=r+1}^{\infty}(1-q^{-j}). \tag{2}$$

The notion of a 'random p-divisible group' having been specified, it remains to ask whether the p-divisible groups of random hyperelliptic Jacobians act like random p-divisible groups. In § 4, we gather some numerical evidence concerning this question. The results are in some sense affirmative, but they display several surprising (to us) features.

For instance, the probability that a random hyperelliptic curve over $\mathbf{F}_3$ is ordinary does not appear to approach the value given in (1). Rather, it is apparently converging to 2/3. However, it does not seem that $\lim_{d\to\infty} P_o(q,d) = 1-1/q$ in general. For instance, $P_o(5,d)$ appears to be converging to $(1-1/5)(1-1/125) = 0.7936$, which is a truncation of the second infinite product in (1). For larger q, the difference between $P_o(q,d)$ and $\prod_{i=1}^{\infty}(1+q^{-i})^{-1}$ is too small to detect reliably from our data. We have no principled

basis to make a conjecture about the precise value $\lim_{d\to\infty} P_o(q,d)$, but our data is certainly consistent with the hypothesis that the limit exists, and that

$$\frac{\log(\lim_{d\to\infty} P_o(p,d) - \prod_{i=1}^{\infty}(1+p^{-i})^{-1})}{\log p} \tag{3}$$

goes to $-\infty$ as p grows.

One might speculate that the discrepancy between experiment and heuristic is a result of our restriction to hyperelliptic curves. What if we consider random curves, or even random principally polarized abelian varieties, more generally? The moduli spaces $\mathcal{M}_g$ and $\mathcal{A}_g$ are both of general type for large g, making it hopeless to sample curves or abelian varieties truly at random. But one can at least study various rationally parameterized families. We find that the proportion of ordinary *plane curves* over $\mathbf{F}_3$ is indistinguishable from $\prod_{i=1}^{\infty}(1+3^{-i})^{-1}$. In other words, *plane curves over* $\mathbf{F}_3$ *are substantially less likely than hyperelliptic curves to be ordinary.* We have no explanation for this phenomenon. The proportion of ordinary plane curves over $\mathbf{F}_2$ does not seem to be $\prod_{i=1}^{\infty}(1+2^{-i})^{-1}$; the data is consistent, though, with the hypothesis that (3) holds for plane curves as well as hyperelliptic curves.

In § 4, we discuss the geometry of various strata in the moduli space of hyperelliptic curves, and what relationship the statistical phenomena observed in § 4 bear to the geometry of these spaces.

2. From p-divisible groups to Dieudonné modules

Let k be a perfect field of characteristic p. We briefly recall the classification of finite flat group schemes of p-power order and of p-divisible groups over k afforded by (covariant) Dieudonné theory. Some general references on these topics are [7, 10], [14, II–III] and [26]. Readers already familiar with this story may skip immediately to the next section.

Let G be a finite commutative k-group scheme of p-power order.[4] We denote by $G^\vee$ the Cartier dual of G, and note that one has a canonical 'double duality' isomorphism $G^{\vee\vee} \simeq G$. We write $F_G\colon G \to G^{(p)}$ and $V_G\colon G^{(p)} \to G$ for the relative Frobenius and Verschiebung morphisms, respectively, and when G is clear from context we will simply write F^r and V^r for the r-fold iterates of relative Frobenius and Verschiebung, defined in the obvious way. Note that, by definition, the composition of F and V in either order is multiplication by p. Since k is perfect, there is a canonical decomposition of G into its étale, multiplicative, and local–local subgroup schemes

$$G = G^{\text{ét}} \times_k G^{\text{m}} \times_k G^{\text{ll}}, \tag{4}$$

which is characterized by the following.

- $G^{\text{ét}}$ is the maximal subgroup scheme of G on which F is an isomorphism.
- G^{m} is the maximal subgroup scheme of G on which V is an isomorphism.
- G^{ll} is the maximal subgroup scheme on which F and V are both nilpotent (in the sense that $F^n = V^n = 0$ for all n sufficiently large).

[4] The *order* of G is by definition $\dim_k(A)$, where $G = \mathrm{Spec}(A)$.

For $\star \in \{\text{ét}, \text{m}, \text{ll}\}$, the formation of $G^\star$ is functorial in G, and there are canonical identifications $(G^{\text{ll}})^\vee \simeq (G^\vee)^{\text{ll}}$, $(G^{\text{m}})^\vee \simeq (G^\vee)^{\text{ét}}$ and $(G^{\text{ét}})^\vee \simeq (G^\vee)^{\text{m}}$.

For a group G of p-power order that is killed by p, the nonnegative integers

$$f = f(G) := \log_p(\text{ord}(G^{\text{ét}})) \quad \text{and} \quad a = a(G) := \dim_k \text{Hom}_{\text{gps}/k}(\alpha_p, G)$$

are called the p-**rank** and a-**number** of G, respectively, where $\alpha_p = \text{Spec}(k[X]/X^p)$ is the unique simple object in the category of p-power order groups over k that are killed by p and are of local–local type.[5] We define the p-**corank** of G to be the difference $\dim(G) - f(G)$.[6] Finally, we say that G is of α-**type** if $G \simeq \alpha_p^m$ for some $m \geqslant 1$.

Remark 2.1. Let G be a k-group of p-power order that is killed by p.

(1) For *any* extension k'/k contained in $\bar{k}$, one has $a(G) = \dim_{k'} \text{Hom}_{\text{gps}/k'}(\alpha_p, G_{k'})$, so the a-number is insensitive to algebraic extension of k.

(2) A finite k-group of p-power order that is killed by p is of α-type if and only if its relative Frobenius and Verschiebung morphisms are both zero. It follows easily from this that G has a unique maximal subgroup of α-type, which we denote by $G[F, V]$. We then have $G[F, V] \simeq \alpha_p^{a(G)}$, so $a(G)$ is the largest integer m for which there exists a closed immersion $\alpha_p^m \hookrightarrow G$ of k-group schemes.

(3) As the inclusion $G^{\text{ét}}(\bar{k}) \hookrightarrow G(\bar{k})$ is an equality, the p-rank of G is the nonnegative integer f for which $|G(\bar{k})| = p^f$, and one will often see the p-rank of G defined this way.

(4) In the special case that $G \simeq G^\vee$, one has $G^{\text{m}} \simeq (G^\vee)^{\text{m}} \simeq (G^{\text{ét}})^\vee$, so also

$$f(G) = \log_p(\text{ord}(G^{\text{m}})) = \dim_{\mathbf{F}_p} \text{Hom}_{\text{gps}/\bar{k}}(\mu_p, G_{\bar{k}}).$$

The right side of the equation above is often used as a definition of $f(G)$ in the literature, since then the definitions for p-rank and a-number look more alike.

Attached to G is its (covariant) **Dieudonné module**, $\mathbf{D}(G)$, which is a finite length $W(k)$-module equipped with a σ-semilinear additive map $F\colon D \to D$ and a σ^{-1}-semilinear additive map $V\colon D \to D$ which satisfy $FV = FV = p$. We view $\mathbf{D}(G)$ as a module over the **Dieudonné ring**: this is the (generally) noncommutative ring A_k generated over $W(k)$ by two indeterminates F and V which satisfy the relations $F\lambda = \sigma(\lambda)F$, $V\lambda = \sigma^{-1}(\lambda)V$ and $FV = VF = p$ for all $\lambda \in W(k)$. If D is *any* (left) A_k-module of finite $W(k)$-length, we define the **dual** of D to be the A_k-module $D^\vee := \text{Hom}_{W(k)}(D, W(k)[1/p]/W(k))$ with[7] $F_{D^\vee} := V_D^\vee$ and $V_{D^\vee} = F_D^\vee$. One checks that

[5] In the definition of a-number, we view the Hom group as a left module over $\text{End}(\alpha_p/k) = k$ in the obvious way.

[6] The *dimension* of G is by definition the k-dimension of the space of invariant differentials on G. The notion of p-corank comes from abelian varieties: is A is an abelian variety over k of dimension g, and $G := A[p]$, then $f(G) \leqslant \dim(G)$, with equality if and only if A is ordinary.

[7] For any $\tau \in \text{Aut}(k)$ and any τ-semilinear additive map $\Psi : D \to D$, we define the *dual* of Ψ to be the τ^{-1}-semilinear additive map $\Psi^\vee : D^\vee \to D^\vee$ whose value on any linear functional $L \in D^\vee$ is the linear functional $\Psi^\vee(L) := \tau^{-1} \circ L \circ \Psi$.

the expected double duality isomorphism $D^{\vee\vee} \simeq D$ (as left A_k-modules) holds. The main theorem of classical Dieudonné theory is as follows.

Theorem 2.2. *The functor $G \rightsquigarrow \mathbf{D}(G)$ from the category of commutative finite k-group schemes of p-power order to the category of left A_k-modules of finite $W(k)$-length is an exact equivalence of abelian categories. Moreover, we have the following.*

(1) *The order of G is p^v, where $v = length_{W(k)}\mathbf{D}(G)$.*

(2) *There is a natural isomorphism of left A_k-modules $D(G^\vee) \simeq D(G)^\vee$.*

(3) *The canonical decomposition $G = G^m \times G^{ét} \times G^{ll}$ corresponds to the canonical decomposition of $D := \mathbf{D}(G)$:*

$$D = D^{ét} \oplus D^m \oplus D^{ll},$$

where $D^\star := \mathbf{D}(G^\star)$ for $\star \in \{ét, m, ll\}$. These A_k-submodules are characterized by the following.

- *$D^{ét}$ is the maximal submodule of D on which V is bijective.*
- *D^m is the maximal submodule of D on which F is bijective.*
- *D^{ll} is the maximal submodule of D on which both V and F are nilpotent.*

(4) *$\mathbf{D}(\alpha_p) = k$ with $V = F = 0$. In particular, if G is killed by p, then $\mathbf{D}(G[F, V])$ is identified with the intersection $\ker V \cap \ker F \subseteq \mathbf{D}(G)$, so $a(G) = \dim_k(\ker V \cap \ker F)$.*

Remark 2.3. It is worth pointing out that, for any automorphism τ of k, the data of a τ-semilinear additive map of $W(k)$-modules $\Psi : D \to D$ is equivalent to the data of a $W(k)$-*linear* map $\Psi^\# : \tau^*D \to D$ for $\tau^*D := D \otimes_{W(k),\tau} W(k)$. Indeed, to Ψ we associate $\Psi^\# := \Psi \otimes 1$, and from $\Psi^\#$ we recover Ψ as the composition of $\Psi^\#$ with the map $D \to \tau^*D$ sending d to $d \otimes 1$. Although some care is necessary, this mechanism will enable us to analyse semilinear algebra structures via the usual methods of linear algebra.

By definition, a ***p*-divisible (= Barsotti–Tate) group over k of height h** is an inductive system $G := \{(G_v, i_v)\}_{v \geqslant 0}$ of finite k-group schemes, with G_v of order p^{hv}, such that

$$0 \longrightarrow G_v \xrightarrow{i_v} G_{v+1} \xrightarrow{p^v} G_{v+1} \longrightarrow 0 \tag{5}$$

is an exact sequence of k-group schemes for all $v \geqslant 0$. The two prototypical examples are $\mathbf{Q}_p/\mathbf{Z}_p := (\mathbf{Z}/p^v\mathbf{Z}, i_v)$ and $\mu_{p^\infty} := (\mu_{p^v}, i_v)$, with i_v the obvious closed immersions in each case. We will be primarily interested in the p-divisible groups associated to abelian varieties: if A/k is an abelian variety, then $A[p^\infty] := (A[p^v], i_v)$ is naturally a p-divisible group, with i_v the canonical closed immersion. We recall that the **dual** of G is by definition the inductive system $G^\vee := (G_v^\vee, j_v^\vee)$ with $j_v : G_{v+1} \to G_v$ the unique map[8] satisfying $i_v \circ j_v = p$. The double-duality isomorphisms at finite level compile to give a canonical isomorphism of p-divisible groups $G^{\vee\vee} \simeq G$ over k. Similarly, the decomposition (4) induces a corresponding splitting $G = G^{\text{ét}} \times_k G^{\text{m}} \times_k G^{\text{ll}}$ with each

[8] This map exists as the exactness of (5) forces the multiplication by p map on G_{v+1} to factor through i_v.

$G^\star$ the inductive system of the $G_v^\star$, and we say that G is étale if $G = G^{\text{ét}}$, and so forth. Furthermore, there are natural identifications $(G^{\text{ll}})^\vee = (G^\vee)^{\text{ll}}$, $(G^{\text{m}})^\vee \simeq (G^\vee)^{\text{ét}}$ and $(G^{\text{ét}})^\vee \simeq (G^\vee)^{\text{m}}$ induced by the ones at finite level.

A **principal quasi-polarization** of a p-divisible group G is an isomorphism $\lambda\colon G \xrightarrow{\simeq} G^\vee$ with the property that the composition $G^{\vee\vee} \to G^\vee$ of the canonical double duality map $G^{\vee\vee} \simeq G$ with λ coincides with $-\lambda^\vee$. A **principally quasi-polarized** (or **pqp** for short) p-divisible group is a pair (G, λ) consisting of a p-divisible group G and a principal quasi-polarization λ. If $G = A[p^\infty]$ for an abelian variety A, then any polarization of degree prime to p on A induces a principal quasi-polarization on G.

The **Dieudonné module** of a p-divisible group $G := \{(G_v, i_v)\}$ is by definition the A_k-module $\mathbf{D}(G) := \varprojlim_{i_v} \mathbf{D}(G_v)$. It follows easily from Theorem 2.2(1) and definitions that $\mathbf{D}(G)$ is free of rank h as a $W(k)$-module. If D is *any* (left) A_k-module that is $W(k)$-finite and free, we define the **dual** of D to be the A_k-module $D^\vee := \text{Hom}_{W(k)}(D, W(k))$ with $F_{D^\vee} := V_D^\vee$ and $V_{D^\vee} := F_D^\vee$, and we define the ***p*-rank, *a*-number** and ***p*-corank** of G to be the corresponding invariants of $G[p] := G_1$. From Theorem 2.2 we obtain the following.

Theorem 2.4. *The functor $G \rightsquigarrow \mathbf{D}(G)$ from the category of p-divisible groups over k to the category of left A_k-modules which are finite and free over $W(k)$ is an equivalence of categories. If $G = \{(G_v, i_v)\}$ is a p-divisible group of height h with Dieudonné module $D = \mathbf{D}(G)$, then the following hold.*

(1) *D is a free $W(k)$-module of rank h, and F, V uniquely determine each other.*

(2) *There is a natural isomorphism of left A_k-modules $\mathbf{D}(G^\vee) \simeq D^\vee$.*

(3) *The canonical decomposition $G = G^m \times G^{ét} \times G^{ll}$ corresponds to the canonical decomposition of D*

$$D = D^{ét} \oplus D^m \oplus D^{ll},$$

where $D^\star := \mathbf{D}(G^\star)$ for $\star \in \{ét, m, ll\}$. These A_k-submodules are characterized by the following.

- *$D^{ét}$ is the maximal submodule of D on which V is bijective.*
- *D^m is the maximal submodule of D on which F is bijective.*
- *D^{ll} is the maximal submodule of D on which V and F are topologically nilpotent.*

(4) *G is pqp if and only if there exists a symplectic* (=perfect, *bilinear, alternating*) *form*

$$\psi_G\colon D \times D \longrightarrow W(k) \quad \text{satisfying} \quad \psi_G(Fx, y) = \sigma(\psi_G(x, Vy)).$$

(5) *Set $\overline{D} = D/pD = \mathbf{D}(G[p])$, and let $\overline{F} := F \bmod p$ and $\overline{V} := V \bmod p$. Then the p-rank of G is the 'infinity rank' of $\overline{V}$, i.e., the k-dimension of the maximal subspace of $\overline{D}$ on which $\overline{V}$ is bijective. The dimension of G is the k-dimension of* $\ker(\overline{V})$. *The a-number of G is the k-dimension of* $\ker \overline{F} \cap \ker \overline{V}$.

Remark 2.5. If G is a pqp p-divisible group over k, then necessarily $G^{\text{m}} \simeq (G^\vee)^{\text{m}} \simeq (G^{\text{ét}})^\vee$, so that G^{m} and $G^{\text{ét}}$ are of the same height. In particular, Theorem 2.4 implies

that the p-rank of G is also the infinity rank of $\overline{F}$ acting on $\overline{D}$, and we will use this fact freely in what follows.

In view of Theorems 2.2 and 2.4, we will often abuse the terminology and say that a Dieudonné module has some property if the corresponding p-divisible group or finite group scheme has this property, and vice versa.

We will be interested in the category BT_1 of commutative group schemes G over k of p-power order that are killed by p which arise as the p-torsion in a Barsotti–Tate group over k. This is equivalent to the condition that the sequence

$$G \xrightarrow{F_G} G^{(p)} \xrightarrow{V_G} G \tag{6}$$

is exact. An object of BT_1 is called a **truncated Barsotti–Tate group of level** 1, or a BT_1 for short. We will write DBT_1 for the category of finite $\mathbf{F}_q$-vector spaces equipped with semilinear additive maps F and V satisfying $FV = VF = 0$ as well as $\mathrm{im}(F) = \ker(V)$ and $\ker(F) = \mathrm{im}(V)$. We note that the Dieudonné module functor restricts to an equivalence of categories $\mathrm{BT}_1 \to \mathrm{DBT}_1$, and that, for example, μ_p and $\mathbf{Z}/p\mathbf{Z}$ are BT_1 s, whereas α_p is not. A **principal quasi-polarization of a $\mathbf{BT}_1$** is a homomorphism $\lambda\colon G \to G^\vee$ with the property that the induced bilinear form $\psi\colon \mathbf{D}(G) \times \mathbf{D}(G) \to k$ on the Dieudonné module of G is symplectic. A **pqp $\mathbf{DBT}_1$** is simply the Dieudonné module of a principally quasi-polarized BT_1.

Remark 2.6. The condition that ψ is symplectic implies that λ is an anti-selfdual isomorphism, i.e., that $\lambda^\vee$ coincides with $-\lambda$ via the double duality identification $G^{\vee\vee} \simeq G$. If $\mathrm{char}(k) \neq 2$, then these two conditions are in fact equivalent. In characteristic 2, however, there exist anti-selfdual isomorphisms $\lambda\colon G \to G^\vee$ which *do not* induce a symplectic form on the Dieudonné module, basically because there are (skew) symmetric forms in characteristic 2 which are not alternating. In general, if $\widetilde{G}$ is a p-divisible group over k prolonging G, then any principal quasi-polarization on $\widetilde{G}$ induces a principal quasi-polarization on G. Our definition of a principal quasi-polarization on a BT_1 is identical to that found in [18, §2.6] and [20, §9.2].

3. Statistics of random Dieudonné modules

In this section, we define a probability distribution on the isomorphism classes of pqp Dieudonné modules (D, F, V, ω) of rank $2g$ over $\mathbf{Z}_q$. To this end, we fix $D = \mathbf{Z}_q^{2g}$, with standard basis $\{e_1, \ldots, e_{2g}\}$ and corresponding standard symplectic form ω corresponding to the matrix

$$\begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix},$$

and we will think of F and V as the entities to be chosen randomly. We will say that a σ-semilinear endomorphism $F\colon D \to D$ is **p-autodual** if there exists a σ^{-1}-semilinear endomorphism $V\colon D \to D$ such that the quadruple (D, F, V, ω) is a pqp Dieudonné

module, or equivalently if $FV = VF = p$ and $\omega(Fx, y) = \sigma(\omega(x, Vy))$ for every $x, y \in D$. Observe that V is uniquely determined by F, if it exists.

For simplicity of notation we say 'σ-endomorphism' (respectively, 'σ-automorphism') to mean 'σ-semilinear endomorphism' (respectively, 'σ-semilinear automorphism'). Suppose that we are given a p-autodual endomorphism F of D. We note first of all that $FD \subset D$ is a subgroup of index q^g containing pD; in particular, the quotient FD/pD is a subgroup of D/pD isomorphic to $(\mathbf{F}_q)^g$. For any $x, y \in D$, we have

$$\omega(Fx, Fy) = \sigma(\omega(x, VFy)) = p\sigma(\omega(x, y)),$$

so that FD/pD is an isotropic (whence maximal isotropic) subspace of the symplectic $\mathbf{F}_q$-vector space D/pD. We denote D/pD by W.

Let F_0 be a p-autodual endomorphism of D. We define $\mathcal{F}(D)$ to be the double coset $\mathrm{Sp}(D)F_0\mathrm{Sp}(D)$, where $\mathrm{Sp}(D)$ is the group of ($\mathbf{Z}_q$-linear) symplectomorphisms. Then $\mathcal{F}(D)$ is endowed with a probability measure by pushforward from Haar measure on the group $\mathrm{Sp}(D) \times \mathrm{Sp}(D)$. Note that every element F of $\mathcal{F}(D)$ is in fact a p-autodual σ-endomorphism of D. We now show that *all* p-autodual σ-endomorphisms arise in this way, which means that $\mathcal{F}(D)$ is independent of our original choice of F_0.

Proposition 3.1. *$\mathcal{F}(D)$ is the set of p-autodual σ-endomorphisms of D.*

Proof. Let F be a p-autodual σ-endomorphism of D. Then FD/pD is a maximal isotropic subspace of W. By the symplectic version of Witt's theorem [4, Theorem 3.9], $\mathrm{Sp}(W)$ acts transitively on the maximal isotropic subspaces, and since $\mathrm{Sp}(D)$ surjects onto $\mathrm{Sp}(W)$, we can choose $g \in \mathrm{Sp}(D)$ such that $gF_0D/pD = FD/pD$. Since FD and gF_0D both contain pD, these two subgroups of D are actually equal. Now F induces an isomorphism from D to FD, so its inverse F^{-1} can be thought of as an isomorphism from FD to D. Thus the composition $F^{-1}gF_0$ is a $\mathbf{Z}_q$-linear automorphism of D which preserves ω; i.e., it is an element g' of $\mathrm{Sp}(D)$. This shows that F lies in $\mathrm{Sp}(D)F_0\mathrm{Sp}(D)$, as claimed. □

By a **random pqp Dieudonné module** (D, F, V, ω) **of dimension** $2g$, we mean one in which F is chosen randomly from $\mathcal{F}(D)$ with respect to the above probability measure, and V is determined from F. When there is no danger of confusion we denote (D, F, V, ω) simply by D.

If X is a statistic of Dieudonné modules (such as a-number, or dimension of the local–local part) we denote by $\mathcal{E}_g(X)$ the expected value of $X(D)$, where D is a random pqp Dieudonné module of rank $2g$. The statistics of interest to us are those where $\mathcal{E}_g(X)$ approaches a limit as $g \to \infty$; in this case, we denote the limit by $\mathcal{E}(X)$ and refer to it as the expected value of X for a random pqp Dieudonné module, the 'large-g limit' being understood. If P is a true-or-false assertion about Dieudonné modules, the 'probability that a random Dieudonné module satisfies P' is understood to mean the expected value of the Bernoulli variable, which is 1 when P holds and 0 otherwise.

We define $\overline{\mathcal{F}}(D)$ to be the reduction of $\mathcal{F}(D)$ modulo p, with its inherited probability distribution. In other words, if $\overline{F}_0$ is the reduction of F_0 to a σ-endomorphism of W, then $\overline{\mathcal{F}}(D)$ is $\mathrm{Sp}(W)\overline{F}_0\mathrm{Sp}(W)$, with the probability distribution obtained by pushforward from

the Haar measure (i.e., the counting measure) on $\mathrm{Sp}(W) \times \mathrm{Sp}(W)$. If F is an element of $\overline{\mathcal{F}}(D)$, then F is a σ-endomorphism of W whose kernel is a maximal isotropic subspace of W. The reduction $\overline{\omega}$ of ω provides an isomorphism $\lambda : W \to W^\vee$ between W and its $\mathbf{F}_q$-linear dual, and we set $V := \lambda^{-1} \circ F^\vee \circ \lambda$. Note that V is then a σ^{-1}-endomorphism of W satisfying $VF = FV = 0$, and that in fact $(W, F, V, \overline{\omega})$ is a pqp DBT_1.

By a **random pqp DBT$_1$** we mean a $\mathrm{DBT}_1(W, F, V)$, endowed with the symplectic form $\overline{\omega}$, obtained as above by choosing a random element of $\overline{\mathcal{F}}(D)$. Statistics of random pqp DBT_1s are again understood to be computed in the large-g limit.

In this paper, we will restrict our attention almost entirely to invariants of p-divisible groups which depend only on the associated DBT_1, such as a-number and p-corank. It should certainly be possible to compute the statistics of more refined invariants (e.g., Newton polygon) but, with the aim of avoiding ungrounded speculation in the context of abelian varieties, we have mostly restricted ourselves to invariants for which we have collected substantial experimental data on Jacobians on curves.

The subspaces $W_1 := \ker F$ and $W_2 := \mathrm{im}\, F$ of W are g-dimensional maximal isotropics, and we denote by F' the σ-isomorphism from W/W_1 to W_2 induced by F. The following proposition provides a useful description of a random pqp DBT_1 in terms of W_1, W_2, and F'.

Proposition 3.2. *Let $(W, F, V, \overline{\omega})$ be a random pqp DBT_1. Then the pair $(W_1, W_2) := (\ker F, \mathrm{im}\, F)$ is uniformly distributed on the set of pairs of maximal isotropic subspaces of W, and F' is uniformly distributed among σ-isomorphisms from (W/W_1) to W_2.*

Proof. The action of $\mathrm{Sp}(W) \times \mathrm{Sp}(W)$ is transitive on pairs of maximal isotropic subspaces, and the probability distribution on $\overline{\mathcal{F}}(D)$ is invariant under this action; this gives the first assertion. Now suppose that we condition on $\ker F = W_1$ and $\mathrm{im}\, F = W_2$; let $\overline{\mathcal{F}}(D, W_1, W_2)$ be the subset of $\overline{\mathcal{F}}(D)$ satisfying this condition. Then $\overline{\mathcal{F}}(D, W_1, W_2)$ is still invariant under left multiplication by the subgroup of $\mathrm{Sp}(W)$ preserving W_2; this subgroup is in fact isomorphic to $\mathrm{GL}(W_2)$ and permutes the choices of F' transitively. This yields the second assertion. □

The definitions given here may seem somewhat unsatisfactory; our 'random DBT_1' is in some sense more like 'a random DBT_1 with a choice of $\mathbf{Z}_q$-basis'. We show below that our definition conforms with a more intrinsic definition of a random DBT_1. The groupoid formalism used here will not return again until the proof of Proposition 3.10.

Definition 3.3. Let G be a finite groupoid; that is, G is a groupoid with finitely many isomorphism classes of objects and finite Hom sets. The *uniform distribution* on G is the unique distribution on isomorphism classes of objects whose mass on an isomorphism class c is inversely proportional to the number of automorphisms of an object in c. We say that a finite set of objects S in G is *uniformly distributed* in G if the probability that a random element of S lies in an isomorphism class c is given by uniform measure.

The desirability of counting objects with weights inversely proportional to the size of their automorphism group has been known at least since Siegel's mass formula; as regards general groupoids, we learned the formalism from Baez and Dolan.

It is clear that an (anti)equivalence between groupoids G_1 and G_2 carries uniform measure on G_1 to uniform measure on G_2. (This is just the groupoid version of the fact that a bijection of sets transports counting measure from one to the other.) Similarly, if S is a finite set with a *free* action of a group Γ, the pushforward from S to S/Γ of uniform measure on S is uniform measure on S/Γ. The following easy proposition records the fact that the same is true in the groupoid setting.

Proposition 3.4. *Let S be a finite set, let Γ be a finite group acting on S, and let S/Γ be the groupoid whose objects are S and whose morphisms from s to s' are group elements γ in Γ such that $\gamma \cdot s = s'$. Then the objects of S are uniformly distributed in S/Γ.*

Proof. The probability that a random s in S lies in the Γ-orbit Γs_0 of a fixed $s_0 \in S$ is precisely

$$|\Gamma s_0|/|S| = 1/\mathrm{Aut}_{S/\Gamma}(s_0). \quad \square$$

We now explain how this formalism applies in the present context. Let $(W, \overline{\omega})$ be a $\mathbf{F}_q$-vector space of dimension $2g$ endowed with a nondegenerate symplectic form. Let S be the set of σ-endomorphisms $F\colon W \to W$ whose kernel is a maximal isotropic subspace of W. Note that S is in bijection with the set of triples (W_1, W_2, F') described in Proposition 3.2; in particular, a random DBT_1 of rank $2g$ is the same thing as a random element of S in uniform distribution.

Now the group $\Gamma = \mathrm{Sp}_{2g}(\mathbf{F}_q)$ acts on S by changes of basis preserving the symplectic form. And the groupoid S/Γ is equivalent to the category of (Dieudonné modules of) principally quasi-polarized BT_1 s. Thus, a random pqp DBT_1, in our sense, is a random principally polarized DBT_1 in the sense of Definition 3.3.

The above discussion is rather formal, but we will see that the groupoid viewpoint is quite convenient in the proof of Proposition 3.10.

The a-number of a random pqp DBT_1

Let (D, F, V) be a DBT_1 over $\mathbf{F}_q$. By Theorem 2.2(4), the a-number of D is the k-dimension of the intersection $\ker F \cap \ker V \subseteq D$; by definition of the category DBT_1, we have $\ker V = \mathrm{im}\, F$, so also $a(D) = \dim_k(\ker F \cap \mathrm{im}\, F)$.

Proposition 3.5. *The probability that $a(D) = r$ is*

$$q^{-\binom{r+1}{2}} \prod_{i=1}^{\infty}(1+q^{-i})^{-1} \prod_{i=1}^{r}(1-q^{-i})^{-1}.$$

Proof. The a-number does not depend on F', so we are computing the probability that two random maximal isotropic subspaces of a large symplectic space over $\mathbf{F}_q$ intersect in a subspace of dimension r.

Let W be a $2g$-dimensional symplectic space. The number of maximal isotropic subspaces in W is

$$\frac{|\mathrm{Sp}_{2g}(\mathbf{F}_q)|}{q^{(1/2)g(g+1)}|\mathrm{GL}_g(\mathbf{F}_q)|} = q^{(1/2)(g^2+g)}\frac{|\mathrm{Sp}_{2g}(\mathbf{F}_q)|}{q^{2g^2+g}}\frac{q^{g^2}}{|\mathrm{GL}_g(\mathbf{F}_q)|}. \tag{7}$$

By the symplectic version of Witt's theorem, the symplectic group $\mathrm{Sp}(W)$ acts transitively on the pairs of maximal isotropic subspaces with r-dimensional intersection; so, to count the number of such pairs, it suffices to compute the size of the stabilizer of such a pair in $\mathrm{Sp}(W)$. Suppose for instance that the pair is given by

$$V_1 = \langle e_1, \ldots, e_g \rangle, \quad V_2 = \langle e_1, \ldots, e_r, e_{g+r+1}, \ldots, e_{2g} \rangle.$$

Then the stabilizer of the pair (V_1, V_2) is the group of matrices of the form

$$\begin{bmatrix} A & B \\ 0 & (A^T)^{-1} \end{bmatrix},$$

where A lies in the parabolic subgroup preserving $\langle e_1, \ldots, e_r \rangle$ and B is symmetric, having zero (i, j) entry when $i > r$ and $j > g + r$. The order of this group is

$$q^{g^2 + \binom{r+1}{2}} \frac{|\mathrm{GL}_r(\mathbf{F}_q)|}{q^{r^2}} \frac{|\mathrm{GL}_{g-r}(\mathbf{F}_q)|}{q^{(g-r)^2}},$$

so the number of pairs of maximal isotropics with r-dimensional intersection is

$$q^{g^2+g-\binom{r+1}{2}} \frac{q^{r^2}}{|\mathrm{GL}_r(\mathbf{F}_q)|} \frac{q^{(g-r)^2}}{|\mathrm{GL}_{g-r}(\mathbf{F}_q)|} \frac{|\mathrm{Sp}_{2g}(\mathbf{F}_q)|}{q^{2g^2+g}}. \tag{8}$$

Dividing (8) by the square of (7) yields

$$q^{-\binom{r+1}{2}} \frac{q^{r^2}}{|\mathrm{GL}_r(\mathbf{F}_p)|} \frac{q^{(g-r)^2}}{|\mathrm{GL}_{g-r}(\mathbf{F}_q)|} \left(\frac{|\mathrm{GL}_g(\mathbf{F}_p)|}{q^{g^2}} \right)^2 \frac{q^{2g^2+g}}{|\mathrm{Sp}_{2g}(\mathbf{F}_q)|},$$

which, as g goes to infinity with r fixed, approaches the desired quantity. □

Remark 3.6. (1) We note that this prediction is in keeping with the fact that the locus of abelian varieties with a-number at least r in $\mathcal{A}_g/\mathbf{F}_q$ has codimension $\binom{r+1}{2}$ and is irreducible if $r < g$; see [23, 3.2] and § 4.

(2) The work of Poonen and Rains [22] posits that the mod p Selmer group of a random quadratic twist of a fixed elliptic curve should be distributed like the intersection of two random maximal isotropics in an *orthogonal* vector space. They show that the mod p Selmer group actually *does* arise as the intersection of two maximal isotropics – the question, then, is whether these isotropics are in fact 'uniformly distributed' in an appropriate sense. Our situation is similar; the a-number of a pqp p-divisible group is indeed the dimension of the intersection of the two maximal isotropics FW and VW in the symplectic vector space W, and one is asking whether these maximal isotropics are distributed uniformly when W arises from an abelian variety.

(3) The conjectured distribution of the a-number is the same as the distribution on the dimension of the fixed space of a random large symplectic matrix over $\mathbf{F}_q$, which was computed in an unpublished work by Rudvalis and Shinoda [24] (see [11] for a review of their results and an alternative proof). This distribution also appears in the conjectures of Malle [16] and Garton [13] as the conjectured distribution of

p-ranks of ideal class groups of number fields containing pth roots of unity. In the class group context, the relationship with the fixed space of a random symplectic matrix is motivated by the analogy between number fields and function fields, where the symplectic matrix describes the action of Frob_ℓ on p-adic cohomology.

The a-number of D is 0 if and only if D is ordinary. We thus have the following corollary.

Corollary 3.7. *The probability that a random pqp Dieudonné module is ordinary is*

$$\prod_{i=1}^{\infty}(1+q^{-i})^{-1}.$$

In problems of Cohen–Lenstra type, it is often the case that moments of variables have a nicer formula than probability distributions do. The present situation is no exception.

Proposition 3.8. *Let $X_m(D)$ be the number of closed immersions of group schemes over $\mathbf{F}_q$ from α_p^m to the p-torsion in the p-divisible group associated to D. Then $\mathcal{E}X_m(D) = q^{\binom{m}{2}}$.*

Proof. In the language of the present paper, we claim that

$$X_m(D) = (q^{a(D)}-1)(q^{a(D)}-q)\cdots(q^{a(D)}-q^{m-1}).$$

Indeed, if G is the p-divisible group attached to D, then any closed immersion $\alpha_p^m \hookrightarrow G[p]$ of group schemes necessarily factors through the maximal α-type subgroup scheme $G[F,V] \simeq \alpha_p^{a(G)}$ of $G[p]$ (see Remark 2.1(2)). In particular, such closed immersions are in bijection with closed immersions $\alpha_p^m \hookrightarrow \alpha_p^{a(G)}$, which are in bijection with injections $\mathbf{F}_q^m \hookrightarrow \mathbf{F}_q^{a(G)}$ via the exact functor $\mathbf{D}(\cdot)$, thanks to Theorem 2.2(4).

Because the distribution of X agrees with the distribution on the dimension of the fixed space of a random matrix g in $\mathrm{Sp}(W)$ (see Remark 3.6 (3)), it suffices to show that the number of injections from an m-dimensional vector space into the fixed space of g has the desired expected value. By Burnside's lemma, this is the same as the number of orbits of $\mathrm{Sp}(W)$ acting on the set of injections $i\colon \mathbf{F}_q^m \hookrightarrow W$. By the symplectic version of Witt's theorem, two such injections i_1, i_2 are in the same orbit if the symplectic forms $i_1^*\langle\rangle$ and $i_2^*\langle\rangle$ agree; so the number of orbits is just the number of alternating bilinear forms on an m-dimensional vector space, which is $q^{\binom{m}{2}}$, as claimed. □

The p-corank of a random pqp $\mathbf{DBT}_1$

Suppose that $X(D)$ is a statistic which is invariant under symplectic change of basis, i.e., under conjugation of F by $\mathrm{Sp}(W)$. As above, by Witt's theorem, all pairs of maximal isotropic subspaces with intersection dimension r are in the same orbit of the symplectic group. Thus, to compute the expected value of $X(D)$ conditional on $a(D)=r$, it suffices to compute the expected value of $X(D)$ for a fixed choice of W_1 and W_2, and F' chosen

uniformly from the σ-isomorphisms from W/W_1 to W_2. The composition

$$\phi\colon W_2 \longrightarrow W \twoheadrightarrow W/W_1 \xrightarrow{F'} W_2$$

is then a σ-endomorphism of W_2 of rank $g-r$, and in fact is chosen uniformly from the set of such σ-endomorphisms.

When $W_2 = \operatorname{im} F$, the σ-endomorphism ϕ is just the map $FW \to FW$ induced by F. In particular, the p-corank of the p-divisible group attached to D is precisely the corank of ϕ^∞.

Proposition 3.9. *Let $0 \leqslant r \leqslant s$ be integers. Then the probability that the a-number of D is r and the p-corank of D is s is*

$$q^{-\binom{r+1}{2}+r-s} \prod_{i=1}^{\infty}(1+q^{-i})^{-1} \prod_{i=r}^{s-1}(1-q^{-i}) \prod_{i=1}^{s-r}(1-q^{-i})^{-1}. \tag{9}$$

Proof. We first show that the probability that a random σ-endomorphism of a g-dimensional vector space V has rank $g-r$ approaches

$$q^{-r^2} \prod_{i=r+1}^{\infty}(1-q^{-i}) \prod_{i=1}^{r}(1-q^{-i})^{-1} \tag{10}$$

as g goes to infinity. Indeed, the map $\phi \mapsto (V \to \operatorname{im}\phi, \operatorname{im}\phi)$ defines a bijection between σ-endomorphisms $\phi\colon V \to V$ of rank $g-r$ and pairs (ψ, W), where $W \in \mathrm{Gr}_{g,g-r}(\mathbf{F}_q)$ is a subspace of V of dimension $g-r$ and $\psi\colon V \to W$ is a σ-semilinear surjection. For a given such W, there are

$$\prod_{i=0}^{g-r-1}(q^g - q^i) \tag{11}$$

such σ-semilinear surjections, by Remark 2.3. Considering the stabilizer of the natural action of GL_g on $\mathrm{Gr}_{g,g-r}$ shows that

$$|\mathrm{Gr}_{g,g-r}(\mathbf{F}_q)| = \frac{|\mathrm{GL}_g(\mathbf{F}_q)|}{|\mathrm{GL}_r(\mathbf{F}_q)||\mathrm{GL}_{g-r}(\mathbf{F}_q)||\mathrm{M}_{r,g-r}(\mathbf{F}_q)|}. \tag{12}$$

Dividing the product of (11) and (12) by $|\mathrm{M}_g(\mathbf{F}_q)|$ yields

$$q^{-r^2}\frac{\prod_{i=0}^{g-r-1}(q^g-q^i)}{q^{(g-r)g}}\frac{q^{r^2}}{|\mathrm{GL}_r(\mathbf{F}_q)|}\frac{q^{(g-r)^2}}{|\mathrm{GL}_{g-r}(\mathbf{F}_q)|}\frac{|\mathrm{GL}_g(\mathbf{F}_q)|}{q^{g^2}},$$

which, as g goes to infinity with r fixed, approaches the quantity of (10).

By [15], for integers $g > s \geqslant r \geqslant 0$ the number of σ-endomorphisms of V such that $\operatorname{rank}(M) = s$ and $\operatorname{rank}(M^\infty) = r$ is

$$\frac{\left(\prod_{i=0}^{r-1}(q^g-q^i)\right)|\mathrm{GL}_{g-r}(\mathbf{F}_q)|\left(\prod_{i=0}^{s-r-1}(q^{g-r-1}-q^i)\right)q^{r(g-r)}}{|\mathrm{GL}_{s-r}(\mathbf{F}_q)|\cdot|\mathrm{GL}_{g-s}(\mathbf{F}_q)|\cdot|\mathrm{M}_{s-r,g-s}(\mathbf{F}_q)|}.$$

It follows that the probability that a random σ-endomorphism of V has $\operatorname{rank}(M^\infty) = g - s$, conditional on $\operatorname{rank}(M) = g - r$, approaches

$$q^{r-s} \prod_{i=r}^{s-1} (1 - q^{-i}) \prod_{i=1}^{r} (1 - q^{-i}) \prod_{i=1}^{s-r} (1 - q^{-i})^{-1} \tag{13}$$

as g approaches infinity. Multiplying (13) by the constant in Proposition 3.5 yields the desired result. □

Summing (9) with s fixed and r between 1 and s gives the probability that the p-corank of D is s; for example, the probability that the corank is 1 is $q^{-1} \prod_{i=1}^{\infty} (1 + q^{-i})^{-1}$, and the probability that the corank is 2 is $(q^{-2} + q^{-3}) \prod_{i=1}^{\infty} (1 + q^{-i})^{-1}$.

The group of $\mathbf{F}_q$-rational points of a random pqp $\mathbf{DBT_1}$

Let G be a BT_1 with Dieudonné module W. The group $G(\mathbf{F}_q)$ of its $\mathbf{F}_q$-rational points is the subgroup of $G(\overline{\mathbf{F}}_q)$ fixed by Frob_q.

Proposition 3.10. *The group of $\mathbf{F}_q$-rational points of the group scheme associated to a random pqp DBT_1 has cardinality p^d with probability*

$$p^{-d^2} \prod_{i=1}^{d} (1 - p^{-i})^{-1} \prod_{j=d+1}^{\infty} (1 - p^{-j}). \tag{14}$$

Proof. We again use the description of ϕ (from the proof of Proposition 3.9) as a random corank-d σ-endomorphism of the g-dimensional vector space FW. Let (X, Y, ϕ_X, ϕ_Y) be a quadruple, where $X \oplus Y = FW$ is a direct sum decomposition, ϕ_X is a nilpotent σ-endomorphism of X with corank d, and ϕ_Y is a σ-automorphism of Y. Then $\phi_X \oplus \phi_Y$ is a corank-d σ-endomorphism of FW. Conversely, any choice of a corank-d σ-endomorphism ϕ yields a quadruple as above by taking Y to be the subspace of FW on which ϕ acts invertibly and X the subspace on which ϕ acts nilpotently. So a uniformly chosen corank-d σ-endomorphism of FW is the same as a uniformly chosen quadruple (X, Y, ϕ_X, ϕ_Y). In particular, the action of F on $F^\infty W$ is precisely ϕ_Y, which is drawn uniformly at random from the set of σ-automorphisms of Y.

Now Y is itself a Dieudonné module, on which F is bijective. Fix a positive integer N. Let $\mathcal{D}_p$ be the category of rank-N p-torsion Dieudonné modules with $\mathbf{F}_q$ coefficients on which F is bijective, $\mathcal{G}_p$ the category of rank-N étale group schemes over $\mathbf{F}_q$ killed by p, and $\mathcal{F}_p$ the category of $N \times N$ matrices over $\mathbf{F}_p$. The morphisms from x to y are, respectively, isomorphisms of Dieudonné modules from x to y; group scheme isomorphisms from x to y; and changes of basis intertwining x and y. All three of these categories are finite groupoids. The functor $G \rightsquigarrow \mathbf{D}(G^\vee)$ provides an antiequivalence of categories $\mathcal{G}_p \simeq \mathcal{D}_p$, while the functor associating to $M \in \mathcal{F}_p$ the étale group scheme G corresponding to the $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$-set $\mathbf{F}_p^N$ with Frob_q-action given by M is an equivalence $\mathcal{F}_p \simeq \mathcal{G}_p$.

The uniformity of ϕ_Y implies by Proposition 3.4 that Y is uniformly distributed in $\mathcal{D}_p$. Thus, the étale group scheme $G_Y/\mathbf{F}_q$ arising from Y via the antiequivalence of $\mathcal{D}_p$ with $\mathcal{G}_p$ is uniformly distributed in $\mathcal{G}_p$, and the matrix M_Y giving the action of Frob_q on $G_Y(\overline{\mathbf{F}}_q)$ is uniformly distributed in $\mathcal{F}_p$. It is precisely the dimension of $\mathrm{coker}(M_Y - 1)$ whose distribution we are trying to study. But applying Proposition 3.4 again, the distribution of $\mathrm{coker}(M_Y - 1)$ for M_Y uniformly distributed in $\mathcal{F}_p$ is identical to the distribution obtained by letting M_Y be a random element of the set $\mathrm{GL}_N(\mathbf{F}_p)$. But the distribution of $\dim \mathrm{coker}(M_Y - 1)$ when M_Y is a random invertible matrix is well known to approach the value (14) as $N = \dim Y \to \infty$. It is easy to see from Proposition 3.9 that $\dim Y$ is larger than any constant multiple of g with probability 1; this finishes the proof. □

Corollary 3.11. *The expected number of surjections from a random pqp BT_1 to the constant group scheme $(\mathbf{Z}/p\mathbf{Z})^d$ is* 1.

We note that the distribution produced here is identical to the Cohen–Lenstra heuristic for the distribution of p-ranks of imaginary quadratic fields. This is quite natural when one considers the p-torsion in the Jacobian of a random hyperelliptic curve C over a finite field. When the field has characteristic p, a heuristic of the form 'random hyperelliptic curves have random pqp DBT_1' would suggest that the finite abelian p-group $\mathrm{Jac}(C)[p](\mathbf{F}_q)$ is distributed according to the Cohen–Lenstra law; in other words, that the conjectural distribution of $\mathrm{Jac}(C)[p](\mathbf{F}_q)$ is exactly the same whether C is defined over a finite field of characteristic p or of characteristic prime to p (as long as the field contains no pth roots of unity).

In the case where C is defined over a finite field k whose characteristic is prime to p, the results of [9] prove that the dth moment in Corollary 3.11 is indeed 1 as long as $|k|$ is sufficiently large relative to p and not congruent to 1 mod p. It would be interesting to see whether there is any way to adapt the methods of [9] to prove that similar statements hold in characteristic p.

Other statistics and questions: final types and Newton polygons

We discuss some further problems which fit into our general framework, but which we have not investigated.

A more refined invariant of a DBT_1 of dimension $2g$ is the **final type**, a g-tuple $\tau = (x_1, \ldots, x_g)$ of non-decreasing integers such that $x_1 \in \{0, 1\}$ and $x_{i+1} \leqslant x_i + 1$. Such a tuple determines the isomorphism class of the corresponding group scheme over an algebraic closure of $\mathbf{F}_q$ and, conversely, any such tuple arises as the final type of a DBT_1; see [23, 2.3]. We note that, unlike the a-number and p-rank, the final type of a DBT_1 depends on F and V, not just their restrictions to the maximal isotropic subspaces $\ker F$ and $\ker V$.

Another invariant of a Dieudonné module D is its Newton polygon: setting $q = p^m$, the **Newton polygon** of D has, for every root α (counted with multiplicity) of the characteristic polynomial of V^m, a segment of slope $\mathrm{ord}_p(\alpha)/m$; when $q = p$, this is just the Newton polygon of the characteristic polynomial of V. The Newton polygon determines D up to isogeny; see [17, II, §4.1]. We note that, unlike the a-number, p-rank,

or the final type, the Newton polygon of a Dieudonné module D is not determined by D/pD. The question of which Newton polygons are compatible with which final types is a subject of active research [21].

Questions. (1) The p-rank of a Dieudonné module is equal to the number of segments of the Newton polygon of slope zero; a natural generalization of Proposition 3.9 is thus the following. For $\lambda \in \mathbf{Q} \cap (0,1)$, let $\mathrm{m}_\lambda(D)$ be the number of segments of slope λ in the Newton polygon of D. Does $\mathrm{m}_\lambda(\cdot)$ converge to a distribution as $g \to \infty$? Moreover, can one compute, for a fixed non-negative integer d, the probability that $\mathrm{m}_\lambda(D) = d$ or the average value of $\mathrm{m}_\lambda(D)$?

(2) More generally, the Newton polygon D of a random Dieudonné module has a local–local part D^{ll} as defined in Theorem 2.2; D^{ll} has rank $2c$, where c is the p-corank of D, and the Newton polygon of D^{ll} has all slopes in the open interval $(0,1)$. Our expectation is that the probability distribution on the Newton polygon of D^{ll}, conditional on the p-corank of D being c, should be given by the probability distribution on Newton polygons of nilpotent p-autodual matrices on $\mathbf{Z}_p^{2c}$. We expect that one can compute this distribution by force for small c.

(3) One can generalize either of these questions by picking, for each g, a subset S_g of the set of possible Newton polygons (respectively, final types) and asking for the proportion of Dieudonné modules whose appropriate invariant lies in S_g. Of course, some conditions on S_g will be necessary to ensure that the proportion approaches a limit. An example where we expect a positive answer would be that in which S_g is the set of final types with $\tau_{g-1} = g - 1 - s$ for a fixed integer s.

4. Random curves, random abelian varieties, and random p-divisible groups

So far, the content of this paper has been purely combinatorial; we have computed moments and distributions of various statistics on random pqp BT_1 s and random p-divisible groups. In practice, pqp p-divisible groups typically arise from motives. In this section, we address the question of whether p-divisible groups arising from random members of a family of abelian varieties are random p-divisible groups in the sense of (15) below.

Let $M_1, M_2, \ldots$ be a family of schemes (or Deligne–Mumford stacks), and let A_i be an abelian scheme over M_i. The three cases we will consider are as follows.

- $M_g = \mathcal{H}_g$, the moduli space of hyperelliptic genus-g curves, and A_g the Jacobian of the universal curve.
- $M_g = \mathcal{M}_g$, and A_g the Jacobian of the universal curve.
- $M_g = \mathcal{A}_g$, and A_g the universal abelian g-fold.

We say that the p-divisible groups associated to such a family are 'random' with respect to a statistic X if

$$\lim_{g\to\infty} \frac{\sum_{y\in M_g(\mathbf{F}_q)} X(A_{g,y}[p^\infty])}{|M_g(\mathbf{F}_q)|} = \mathcal{E}X. \tag{15}$$

Which of these families, with respect to which statistics, yield random p-divisible groups? In this section, we discuss the numerical evidence concerning this question, and some geometric properties of strata of moduli spaces in characteristic p which seem closely related to the statistics in the first part of the paper.

Relation with geometry of moduli spaces

In this short section, we record some remarks about the relationship between the heuristics presented here and the cohomology of moduli spaces of curves and abelian varieties in positive characteristic. There are no theorems in this section, only suggestive relationships between conjectures.

The prediction that the mod p Dieudonné module of the Jacobian of a random hyperelliptic curve over $\mathbf{F}_q$ is a random pqp DBT_1 implies, in particular, that

$$\lim_{g\to\infty} \mathcal{H}_g^{\mathrm{no}}(\mathbf{F}_q)/\mathcal{H}_g(\mathbf{F}_q) \to 1 - \prod_{i=1}^{\infty}(1+q^{-i})^{-1} = 1/q + 1/q^3 + 1/q^4 + \cdots, \tag{16}$$

where $\mathcal{H}_g^{\mathrm{no}}$ denotes the non-ordinary locus, a divisor in $\mathcal{H}_g$. (One can make an analogous guess with $\mathcal{M}_g$ in place of $\mathcal{H}_g$.) Thus, the heuristic goes hand in hand with a belief that the non-ordinary locus is an *irreducible* divisor, at least for all sufficiently large g; otherwise, the ratio would have leading term n/q instead of $1/q$, where n is the number of $\mathbf{F}_q$-rational components of $\mathcal{H}_g^{\mathrm{no}}$.

We emphasize that almost nothing is known about the irreducibility of the non-ordinary locus in $\mathcal{H}_g$ or $\mathcal{M}_g$ (see [2, §3.2] and [3, §3.7]). The non-ordinary locus in $\mathcal{A}_g$, by contrast, is known to be irreducible.

For a family of curves over $\mathbf{F}_q$ with random p-divisible groups, Proposition 3.9 shows that the proportion of curves with a-number r and p-corank s has leading term $q^{-\binom{r+1}{2}+r-s}$, which suggests that the locus of curves with a-number r and p-corank s is an irreducible locally closed subvariety of codimension $\binom{r+1}{2} + r - s$. This is in fact the codimension in $\mathcal{A}_g$ of the locus of abelian varieties with a-number r and p-corank s (see [23, 2.3]); so the heuristics arising from random Dieudonné modules can be read as supportive of (or supported by) the expectation that various natural loci of curves intersect the strata in $\mathcal{A}_g/\mathbf{F}_q$ with the expected dimension.

The heuristic (16) can also be used to make guesses about the cohomology of various strata in $\mathcal{H}_g$ and $\mathcal{M}_g$. For example, suppose that the restriction map from the cohomology of $\mathcal{M}_g$ to the cohomology of the closed subscheme $\mathcal{M}_g^{\mathrm{no}}$ were an isomorphism in some large range. Then one might expect the ratio $\mathcal{M}_g^{\mathrm{no}}(\mathbf{F}_q)/\mathcal{M}_g(\mathbf{F}_q)$ to be very close to $1/q$, contrary to what the heuristic predicts. *Proving* any implication of this kind is well out of reach: the Betti numbers of $\mathcal{M}_g$ grow superexponentially in g, so even with control of the cohomology groups in some large range there is no hope of using Weil bounds to get a good approximation to $\mathcal{M}_g(\mathbf{F}_q)$ [8].

For hyperelliptic curves, the situation is a bit more legible. For simplicity, write $X_n/\mathbf{F}_p$ for the configuration space parameterizing monic degree-n squarefree polynomials $f(x)$,

and let X_n^{no} be the closed subscheme parameterizing those polynomials such that the hyperelliptic curve

$$y^2 = f(x)$$

is non-ordinary. It is easy to check that $|X_n(\mathbf{F}_q)| = q^n - q^{n-1}$ when $n \geqslant 1$; moreover, the étale cohomology of X_n is concentrated in degrees 0 and 1.

If (16) holds, we would have

$$X_n^{\mathrm{no}}(\mathbf{F}_q) \sim (q^n - q^{n-1})(1/q + 1/q^3 + 1/q^4 + \cdots) = q^{n-1} - q^{n-2} + q^{n-3} \cdots .$$

This suggests that X_n^{no} has cohomology beyond the classes pulled back from X_n; for instance, there should be a cohomology class in some even degree generating a subspace on which Frobenius acts with trace q^{n-3}. Moreover, this class might be expected to vanish when char $\mathbf{F}_q = 3$, since the numerical data below suggests that in characteristic 3 the proportion of non-ordinary hyperelliptic curves is precisely $1/q$.

Problem. Construct such a class in the locus of non-ordinary hyperelliptic curves.

Corollary 3.11 says that, on average, a random DBT_1 admits a single surjection to $(\mathbf{Z}/p\mathbf{Z})^d$. Thus, in a family of curves $X$with random p-divisible group, parameterized by a moduli scheme M, the average number of surjections from $\mathrm{Jac}(X)(\mathbf{F}_q)$ to $(\mathbf{Z}/p\mathbf{Z})^d$ is 1. This suggests that the moduli space $M_{p,d}$ is irreducible, where $M_{p,d}$ is the moduli space parameterizing curves X in M together with a level structure $\mathrm{Jac}(X) \to (\mathbf{Z}/p\mathbf{Z})^d$. And this irreducibility for every d suggests that the monodromy representation of the moduli space of ordinary curves in M on the g-dimensional space of étale p-torsion in $\mathrm{Jac}(X)$ has image containing $\mathrm{SL}_g(\mathbf{F}_p)$. In fact, one could refine Corollary 3.11 to apply under supplementary conditions on p-corank, a-number, etc., and the result would be a prediction that, on any of these characteristic p strata, the monodromy in the étale p-torsion of $\mathrm{Jac}(X)$ has full image. In fact, such theorems are already known in the case $M = \mathcal{M}_g$ [2] and $M = \mathcal{H}_g$ [3, §3.7]. It seems reasonable to hope that the results of the those two papers could be used to prove that random hyperelliptic curves and random curves satisfy a weak version of the heuristic suggested by Corollary 3.11, where a limit $q \to \infty$ is taken prior to the limit $g \to \infty$. This would be exactly analogous to the method used by Achter in [1] to derive a similarly weakened Cohen–Lenstra conjecture from a large-monodromy theorem in ℓ-adic cohomology.

Experiments

The tables below contain experimental information about the distribution of a-numbers and orders mod p of Jacobians of hyperelliptic and plane curves.

The constants appearing in the tables are defined as follows. As in Proposition 3.5, we define the constant $\mathrm{MG}(q, r)$ to be

$$\mathrm{MG}(q, r) := q^{-\binom{r+1}{2}} \prod_{i=1}^{\infty} (1 + q^{-i})^{-1} \prod_{i=1}^{r} (1 - q^{-i})^{-1}.$$

Similarly, for a finite group G of p-power order, we define the **Cohen–Lenstra probability** to be

$$C_p(G) := \frac{1}{|\mathrm{Aut}(G)|} \prod_{j=1}^{\infty} (1 - p^{-j}),$$

and, finally, we define the **truncated Malle–Garton constant** to be

$$\mathrm{TMG}(q; b) := \prod_{j=1}^{b} (1 - q^{1-2j}).$$

Table 1 contains distributions of a-numbers of Jacobians of hyperelliptic curves; we explain below how the computations were done. As noted in the introduction, the data suggests that the probability that the Jacobian of a random hyperelliptic curve has a-number 0 does not approach the value given by our heuristics. Rather, for $q = 3$ the data suggests that the true probability is $2/3 = \mathrm{TMG}(3; 1)$, and for $q = 5$ it suggests $0.7936 = \mathrm{TMG}(5; 2)$. To verify this, for $q = 5$ we took exhaustive data for low g (i.e., computed the a-number of the Jacobian of *every* hyperelliptic curve of genus g). For larger g it is unreasonable to do an exhaustive computation; for $g = 21$ we computed the a-numbers of the Jacobians of 819200000 random hyperelliptic curves, and indeed the proportion which were ordinary was closer to the truncated constant. For $q > 5$, we did not generate enough data to distinguish between the Malle–Garton constant and the truncated variant.

It is natural to ask what the 'truncated' version of $\mathrm{MG}(q, r)$ should be for larger values of r. For instance, the proportion of hyperelliptic curves over $\mathbf{F}_3$ with a-number 1 appears to converging to a value $0.296\ldots$. What limiting value (presumably a power series in $1/3$) is suggested by this experimental result?

Table 2 contains distributions of a-numbers of Jacobians of plane curves. The sample sizes are necessarily smaller than those of Table 1 (see the comments in the next section). The data for $q > 2$ agrees well with our heuristics, and in particular the truncation phenomenon disappears (or the discrepancy from heuristics is too small for us to measure). For $q = 2$, the data does not agree with our heuristics, and for this fact we have no conceptual explanation. In particular, we do not see an explanation for this discrepancy along the lines of Theorem 4.2 below.

Table 3 (respectively, Table 4) contains the proportion of hyperelliptic curves (respectively, plane curves) C such that $p \nmid |\mathrm{Jac}_C(\mathbf{F}_q)|$ (where $p = \mathrm{char}\, \mathbf{F}_q$). For $q \neq 2$ (respectively, $p > 2$), the data is consistent with the heuristics suggested by Proposition 3.10. For C hyperelliptic, since one can efficiently compute the zeta function of Jac_C (and can thus detect when p exactly divides $|\mathrm{Jac}_C(\mathbf{F}_q)|$), we also report the probability that $\mathrm{Jac}_C[p^\infty](\mathbf{F}_q) \cong \mathbf{Z}/p\mathbf{Z}$.

Remark 4.1. We find in table 4 a notable divergence between experiment and heuristic for smooth plane curves in characteristic 2; it appears that, for plane curves X of odd degree over $\mathbf{F}_q$ with $q = 2^m$, the order of $\mathrm{Jac}(X)(\mathbf{F}_q)$ is almost always even. This was puzzling to us until we realized that the behaviour had a natural explanation, so natural

q	Genus	Sample size	a	Proportion	MG(q,a)	TMG$(p;\frac{p-1}{2})$
3	25	40960000	0	0.666716	0.639005	0.666666
			1	0.296272	0.319502	
			2	0.0328910	0.0399378	
	100	5120000	0	0.666497	0.639005	0.666666
			1	0.296487	0.319502	
			2	0.0329145	0.0399378	
5	5	exhaustive	0	0.793278	0.793335	0.793600
	6	exhaustive	0	0.793875		
	7	exhaustive	0	0.793557		
	21	819200000	0	0.793838	0.793335	0.793600
	25	40960000	0	0.793529	0.793335	0.793600
			1	0.198172	0.198334	
			2	0.00822029	0.00826392	
	100	5120000	0	0.793838	0.793335	0.793600
			1	0.197818	0.198334	
			2	0.00826679	0.00826392	
7	25	40960000	0	0.854542	0.854593	0.854594
			1	0.142490	0.142432	
			2	0.00295969	0.00296733	
9	25	12735000	0	0.888970	0.887655	0.888889
			1	0.109666	0.110957	
			2	0.00134582	0.00138696	
	100	15500	0	0.888774	0.887655	0.888889
			1	0.109871	0.110957	
			2	0.00135484	0.00138696	
25	25	12640000	0	0.959962	0.959939	0.959939
			1	0.0399742	0.0399975	
			2	6.43987E-5	6.40985E-5	
	100	1036000	0	0.959822	0.959939	0.959939
			1	0.0401110	0.0399975	
			2	6.75676E-5	6.40985E-5	
27	25	13030000	0	0.962955	0.962914	0.962963
			1	0.0369945	0.0370352	
			2	5.07291E-5	5.08724E-5	
	100	1044000	0	0.962741	0.962914	0.962963
			1	0.0372021	0.0370352	
			2	5.74713E-5	5.08724E-5	
49	25	20480000	0	0.979568	0.979583	0.979583
81	25	20480000	0	0.987662	0.987653	0.987655
125	25	20480000	0	0.991984	0.991999	0.991999

TABLE 1. Distribution of a-numbers of Jacobians of hyperelliptic curves.

that in fact we can prove that the behaviour persists for plane curves of every odd degree.

Theorem 4.2. *Let d be a positive odd integer, let k be a finite field of characteristic 2, and let $F \in k[X,Y,Z]$ be a homogeneous degree- d form cutting out a smooth curve X in*

q	Degree	Genus	a	Sample size	Proportion	MG(q, a)
2	7	15	0	56949615	0.426022	0.419422
			1		0.422294	0.419422
			2		0.109071	0.139807
	10	36	0	80000	0.423363	0.419423
3	7	15	0	3062000	0.638947	0.639006
			1		0.319267	0.319502
			2		0.0404950	0.0399378
	8	21	0	249230	0.638133	0.639006
	10	36	0	154000	0.639273	0.639006
			1		0.318792	0.319502
			2		0.0404481	0.0399378
4	7	15	0	2782000	0.737809	0.737513
			1		0.245737	0.245837
			2		0.0152703	0.0163892
	10	15	0	521000	0.739500	
			1		0.242875	
			2		0.0174167	
5	7	15	0	590000	0.793784	0.793335
	10	36	0	17851	0.796874	0.793335
9	7	15	0	1080000	0.887926	0.887654
			1		0.110636	0.110957
			2		0.00143426	0.00138696
	10	36	0	102000	0.888040	
			1		0.110549	
			2		0.00140196	
25	7	15	0	563000	0.960135	0.959938
			1		0.0398114	0.0399975
			2		5.33808E-5	6.40985E-5
	10	36	0	36000	0.958667	
			1		0.0412778	
			2		5.55555E-5	
27	7	15	0	947000	0.962757	0.962914
			1		0.0371953	0.0370352
			2		4.75185E-5	5.08724E-5
	10	36	0	89000	0.962023	
			1		0.0378652	
			2		0.000112360	

TABLE 2. Distribution of a-numbers of Jacobians of plane curves.

$\mathbf{P}^2/k$. *Suppose furthermore that at least one monomial* $X^aY^bZ^c$ *with two odd exponents has non-zero coefficient in* F. *Then* $|Jac(X)(k)|$ *is even. In particular, the proportion of smooth degree-* d *plane curves* X/k *with* $|Jac(X)(k)|$ *even goes to* 1 *as* d *goes to* ∞.

Proof. Let ℓ_1, ℓ_2 be distinct linear forms, and let ω be the exact differential $d(\ell_1/\ell_2)$ on X. The divisor of ω is automatically a square, since locally one is just computing the derivative of a Laurent series in $k((t))$, and all such derivatives lie in the field of squares

q	Genus	$\lvert\mathrm{Jac}[p^\infty](\mathbf{F}_q)\rvert$	Sample size	Proportion	$C_p(G)$
3	12	p	20000	0.280100	0.280063
	20	1	1600000	0.560527	0.560126
	25	1	400000	0.560198	0.560126
5	8	p	5000	0.193200	0.190083
	15	1	1600000	0.759874	0.760333
	25	1	400000	0.760077	0.760333
7	15	1	1600000	0.837408	0.836796
	25	1	400000	0.836867	0.836796
9	12	1	274016000	0.560169	0.560126
11	15	1	1600000	0.900908	0.900833
	25	1	400000	0.900988	0.900833
25	12	1	269210000	0.760389	0.760333

TABLE 3. Distribution of $\lvert\mathrm{Jac}[p^\infty](\mathbf{F}_q)\rvert$ for Jacobians of hyperelliptic curves.

q	Degree	Genus	Sample size	Proportion	$C_p(1)$
2	7	15	37940000	0.071762	0.288788
	8	21	1777100	0.229230	
	9	28	313000	0.000223	
	10	36	349500	0.246071	
	11	55	312000	0.0000064	
3	7	15	137000	0.553302	0.560126
	10	36	142000	0.559676	
4	9	28	47775	0.000000	0.288788
	10	36	31200	0.285673	
5	7	15	350000	0.760462	0.760332
	10	36	48000	0.761500	
8	7	15	219725	0.000000	0.288788
	8	21	89575	0.283349	
9	10	36	57000	0.558772	0.560126

TABLE 4. Probability that $p \nmid \lvert\mathrm{Jac}[p^\infty](\mathbf{F}_q)\rvert$ for Jacobians of plane curves.

$k((t^2))$. Let D be the divisor such that $2D = \mathrm{div}(\omega)$; then D is evidently a half-canonical divisor, and its divisor class is independent of the choice of ω (see, e.g., [25, §3].)

On the other hand, the canonical class on a degree-d plane curve is $(d-3)$ times the hyperplane class. Thus, the divisor $(1/2)(d-3)\mathrm{div}(\ell_2)$ is also a half-canonical. The difference between these two half-canonicals is a 2-torsion point on $\mathrm{Jac}(X)(k)$; it remains to show that this point is non-zero under the given conditions.

Note that $D - (1/2)(d-3)\mathrm{div}(\ell_2)$ is principal if and only if the principal divisor $\mathrm{div}(\omega) - (d-3)\mathrm{div}(\ell_2)$ is the divisor of a function $f \in (k(X)^*)^2$. Moreover, a direct

computation shows that $\mathrm{div}(\omega) - (d-3)\mathrm{div}(\ell_2)$ is the divisor of the function

$$\frac{dF}{d\ell_1}\ell_2^{1-d},$$

which is a square only if $dF/d\ell_1$ is the square of a homogeneous form of degree $(1/2)(d-1)$. It is easy to see that this is equivalent to the failure of the condition in the theorem. □

We remark that the converse to Theorem 4.2 does not hold; even when the two half-canonicals constructed in the proof do agree, there is no reason there might not be another $\mathbf{F}_q$-rational 2-torsion point on $\mathrm{Jac}(X)$.

Methods of computation

Let C be a curve over $\mathbf{F}_q$, and let $(W, F, V, \overline{\omega})$ be the pqp DBT_1 associated to the p-torsion subgroup scheme of the Jacobian of C. Then there exists a canonical isomorphism $W \cong H^1_{\mathrm{dR}}(C)$ such that the induced action of F (respectively, V) on $H^1_{\mathrm{dR}}(C)$ is equal to the action of Frobenius (respectively, the Cartier operator) [19, § 5], and $\overline{\omega}$ agrees with the cup product pairing. The actions of F and V respect the Hodge filtration

$$0 \longrightarrow H^0(X, \Omega^1_C) \longrightarrow H^1_{\mathrm{dR}}(C) \longrightarrow H^1(C, \mathcal{O}_C) \longrightarrow 0.$$

Moreover, the action of F on $H^0(X, \Omega)$ is visibly trivial and, dually, $V(H^1_{\mathrm{dR}}(C)) = H^0(X, \Omega)$; in particular, there exists a basis of $H^1_{\mathrm{dR}}(C)$ with respect to which the semilinear maps F and V correspond to the matrices

$$\begin{bmatrix} 0 & B \\ 0 & D \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} A & C \\ 0 & 0 \end{bmatrix}, \tag{17}$$

where $A, B, C, D \in \mathrm{M}_g(\mathbf{F}_q)$. Since $\ker V = \mathrm{im}\, F$, it follows that $a(W) = \dim(\ker F \cap \ker V)$ is equal to the nullity of A; by duality, this is the same as the nullity of D.

The matrix A is called the **Cartier–Manin matrix** of C. When C is a hyperelliptic curve with affine equation $y^2 = f(x)$, there exists a basis of $H^1_{\mathrm{dR}}(C)$ with respect to which A is given by the explicit formula (c_{pi-j}), where $f(x)^{\frac{p-1}{2}} = \sum c_k x^k$ and $p = \mathrm{char}\, \mathbf{F}_q$; see [27] for details. In particular, one can quickly compute the Cartier–Manin matrix, and thus the a-number, of a hyperelliptic curve.

Moreover, one can efficiently compute $|\mathrm{Jac}_C(\mathbf{F}_q)| \bmod p$ (where $q = p^r$) from the Cartier–Manin matrix. Indeed, $|\mathrm{Jac}_C(\mathbf{F}_q)| = P(1)$, where P is the characteristic polynomial of the rth power of Frobenius acting on $H^1_{\text{ét}}(C; \mathbf{Q}_\ell)$ for any $\ell \neq p$; P has integral coefficients and its reduction mod p is equal to the characteristic polynomial of the rth power of Frobenius acting on $H^1_{\mathrm{dR}}(C)$. Choosing a basis so that the matrix corresponding to F is as in (17), F^r will be of the form

$$F^r = \begin{bmatrix} 0 & B' \\ 0 & D' \end{bmatrix}, \quad D' = D \cdot \sigma(D) \cdots \sigma^{r-1}(D),$$

and it thus suffices to compute the value of the characteristic polynomial of D' at 1. We can therefore quickly compute the order of $\mathrm{Jac}_C(\mathbf{F}_q)$ mod p from the Cartier–Manin matrix of C.

When C is a plane curve, we do not know of an explicit formula for A or D in terms of the coefficients of the defining equations of C. There is however an algorithm, implemented as Magma's `CartierRepresentation` function, which, for a particular curve C, computes a representative of A. This computation is much slower than in the hyperelliptic case; accordingly, the sample sizes are smaller for plane curves.

Magma code which performs these computations can be found at the Arxiv page for this paper or at the third author's web page [5].

Acknowledgements. We would like to thank Jeff Achter, Derek Garton, Tim Holland, Bjorn Poonen, and Rachel Pries for useful conversations about the material of this paper.

References

1. Jeffrey D. Achter, The distribution of class groups of function fields, *J. Pure Appl. Algebra* **204**(2) (2006), 316–333, MR 2184814 (2006h:11132).
2. Jeffrey D. Achter and Rachel Pries, Monodromy of the p-rank strata of the moduli space of curves, *Int. Math. Res. Not. IMRN* **15** (2008), Art. ID rnn053, 25; MR 2438069 (2009i:14030).
3. J. D. Achter and R. Pries, The p-rank strata of the moduli space of hyperelliptic curves, *Adv. Math.* (2011).
4. E. Artin, *Geometric algebra* (Interscience Publishers, Inc., New York-London, 1957), MR 0082463 (18,553e).
5. Bryden Cais, Jordan Ellenberg and David Zureick-Brown, Electronic transcript of computations for the paper 'Random Dieudonné modules, random p-divisible groups, and random curves over finite fields', Available at http://www.mathcs.emory.edu/~dzb/. (Also attached at the end of the tex file).
6. H. Cohen and H. Lenstra, Heuristics on class groups of number fields, *Number Theory Noordwijkerhout 1983* (1984), 33–62.
7. Michel Demazure, Lectures on p-divisible groups, Lecture Notes in Mathematics, Volume 302 (Springer, Berlin, 1972), MR 0344261 (49 #9000).
8. A. Johan de Jong and Nicholas M. Katz, Counting the number of curves over a finite field, 2000, preprint.
9. Jordan S. Ellenberg, Akshay Venkatesh and Craig Westerland, Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields 2, 2012, preprint.
10. Jean-Marc Fontaine, *Groupes p-divisibles sur les corps locaux.* (Société Mathématique de France, Paris, 1977), Astérisque, No. 47-48, MR 0498610 (58 #16699).
11. Jason Fulman, A probabilistic approach to conjugacy classes in the finite symplectic and orthogonal groups, *J. Algebra* **234**(1) (2000), 207–224, MR 1799484 (2002j:20094).
12. E. Friedman and L. C. Washington, On the distribution of divisor class groups of curves over a finite field, in *Théorie des nombres (Quebec, PQ, 1987)*, pp. 227–239 (de Gruyter, Berlin, 1989).
13. Derek Garton, Random matrices and the Cohen–Lenstra statistics for global fields with roots of unity, 2012, UW-Madison thesis, in preparation.

14. Alexandre Grothendieck, *Groupes de Barsotti–Tate et cristaux de Dieudonné*. 1974) (Les Presses de l'Université de Montréal, Montreal, Que., Séminaire de Mathématiques Supérieures, No. 45 (Été, 1970), MR 0417192 (54 #5250).
15. Timothy Holland, Counting semilinear endomorphisms over finite fields, 2011.
16. Gunter Malle, On the distribution of class groups of number fields, *Experiment. Math.* **19**(4) (2010), 465–474, MR 2778658 (2011m:11224).
17. Ju. I. Manin, Theory of commutative formal groups over fields of finite characteristic, *Uspehi Mat. Nauk* **18**(6 (114)) (1963), 3–90, MR 0157972 (28 #1200).
18. Ben Moonen, Group schemes with additional structures and Weyl group cosets, in *Moduli of abelian varieties (Texel Island, 1999)*, Progr. Math., Volume 195, pp. 255–298 (Birkhäuser, Basel, 2001), MR 1827024 (2002c:14074).
19. Tadao Oda, The first de Rham cohomology group and Dieudonné modules, *Ann. Sci. École Norm. Sup.* (4) **2** (1969), 63–135, MR 0241435 (39 #2775).
20. Frans Oort, A stratification of a moduli space of abelian varieties, in *Moduli of abelian varieties (Texel Island, 1999)*, Progr. Math., Volume 195, pp. 345–416 (Birkhäuser, Basel, 2001), MR 1827027 (2002b:14055).
21. Frans Oort, Foliations in moduli spaces of abelian varieties, *J. Amer. Math. Soc.* **17**(2) (2004), 267–296 (electronic), MR 2051612 (2005c:14051).
22. Bjorn Poonen and Eric Rains, Random maximal isotropic subspaces and Selmer groups, *J. Amer. Math. Soc.* **25**(1) (2012), 245–269, MR 2833483.
23. Rachel Pries, A short guide to p-torsion of abelian varieties in characteristic p, in *Computational arithmetic geometry*, Contemp. Math., Volume 463, pp. 121–129 (Amer. Math. Soc., Providence, RI, 2008), MR 2459994 (2009m:11085).
24. A. Rudvalis and K. Shinoda, An enumeration in finite classical groups, 1988, preprint.
25. Karl-Otto Stöhr and José Felipe Voloch, A formula for the Cartier operator on plane algebraic curves, *J. Reine Angew. Math.* **377** (1987), 49–64, MR 887399 (88g:14026).
26. J. T. Tate, p-divisible groups, in *Proc. Conf. Local Fields (Driebergen, 1966)*, pp. 158–183 (Springer, Berlin, 1967), MR 0231827 (38 #155).
27. Noriko Yui, On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$, *J. Algebra* **52**(2) (1978), 378–410, MR 0491717 (58 #10920).