New York Journal of Mathematics

New York J. Math. **27** (2021) 705–739.

On BT_1 group schemes and Fermat curves

Rachel Pries and Douglas Ulmer

Abstract. Let p be a prime number and let k be an algebraically closed field of characteristic p. A BT_1 group scheme over k is a finite commutative group scheme which arises as the kernel of p on a p-divisible (Barsotti–Tate) group. We compare three classifications of BT_1 group schemes, due in large part to Kraft, Ekedahl, and Oort, and defined using words, canonical filtrations, and permutations. Using this comparison, we determine the Ekedahl–Oort types of Fermat quotient curves and we compute four invariants of the p-torsion group schemes of these curves.

Contents

1. Introduction

Fix a prime number p and let k be an algebraically closed field of characteristic p. Suppose C is a smooth irreducible projective curve of genus g over k. Its Jacobian $\mathrm{Jac}(C)$ is a principally polarized abelian variety of dimension g. The p-torsion group scheme $G = \mathrm{Jac}(C)[p]$ is a polarized BT_1 group

Received February 9, 2021.

2010 *Mathematics Subject Classification.* Primary 11D41, 11G20, 14F40, 14H40, 14L15; Secondary 11G10, 14G17, 14K15, 14H10.

Key words and phrases. Curve, finite field, Jacobian, abelian variety, Fermat curve, Frobenius, Verschiebung, group scheme, Ekedahl–Oort type, de Rham cohomology, Dieudonné module.

ISSN 1076-9803/2021

scheme of rank p^{2g}. The isomorphism class of G is uniquely determined by the de Rham cohomology of C [Oda69].

An important way to describe the isomorphism class of G is via a combinatorial invariant called the *Ekedahl–Oort type*, or E–O type. The E–O type is a sequence $[\psi_1, \dots, \psi_g]$ of integers such that $\psi_i - \psi_{i-1} \in \{0, 1\}$ for $1 \leq i \leq g$ (letting $\psi_0 = 0$). The p-rank and a-number of G can be quickly computed from the E–O type. The E–O type gives key information about the stratification of the moduli space of principally polarized abelian varieties of dimension g.

Recently, there has been a lot of interest in studying p-torsion group schemes for curves, for example [Moo04], [EP13], [PW15], [DH], and [Moo20]. Despite this, there are very few examples of curves for which the Ekedahl–Oort type has been computed. In this paper, our main result is Theorem 7.1, in which we determine the Ekedahl–Oort type for the Jacobian J_d of the smooth projective curve $\mathcal{C}_d$ with affine equation $y^d = x(1-x)$, for all positive integers d that are relatively prime to p.

Here is our motivation for studying the curve $\mathcal{C}_d$. First, it is a quotient of the Fermat curve F_d of degree d. There has been a lot of work on p-divisible groups of Fermat curves. For example, Yui determined their Newton polygons [Yui80, Thm. 4.2]. Several authors studied the p-ranks and a-numbers of Fermat curves, e.g., [KoW88], [Gon97], and [MonS18]. It turns out that most of the interesting features of the p-torsion group scheme for F_d are already present for that of $\mathcal{C}_d$.

Second, the de Rham cohomology of $\mathcal{C}_d$, with its Frobenius and Verschiebung operators, has a streamlined description. Typically it is complicated to discern the Ekedahl–Oort type from a computation of these operators. In the case of $\mathcal{C}_d$, the actions of F and V are given by permutation data that is easy to analyze. For this reason, we are able to describe the mod p Dieudonné module of $J_d[p]$ in several different ways and give a closed form formula for its Ekedahl–Oort type.

Third, in our companion paper [PU], we prove that every polarized BT_1-group scheme over k occurs as a direct factor of the p-torsion group scheme of J_d for infinitely many d as long as $p > 3$. In other words, the class of curves $\mathcal{C}_d$ for $p \nmid d$ includes all possible structures of p-torsion group schemes of principally polarized abelian varieties.

To prove Theorem 7.1, we rely on a detailed comparison of three classifications of BT_1 group schemes, essentially due to Kraft, Ekedahl, and Oort. We develop this comparison in Sections 2 through 4, working in general, not restricting to Jacobians of curves. The Kraft classification uses words on a two-letter alphabet $\{f, v\}$; it interacts well with direct sums and identifies the indecomposable objects in the category. The Ekedahl–Oort classification uses the interplay between F and V to build a "canonical filtration" and is well suited to moduli-theoretic questions. The third classification is given in terms of a finite set S with a permutation and a partition into two subsets, and it is particularly well suited to studying Fermat curves. The material in these sections is fundamental to the proof of the theorem and does not appear in a self-contained way elsewhere in the literature.

In Section 5, we study homomorphisms between BT_1 group schemes to analyze two well-known invariants, the p-rank and a-number, and two newer invariants related to the p-torsion group scheme of a supersingular elliptic curve, called the $s_{1,1}$-multiplicity and $u_{1,1}$-number.

In Section 6, we recall two results about the BT_1 modules of Fermat curves and their quotients from [PU]. In Section 7, we prove the main result about the Ekedahl–Oort type of $\mathcal{C}_d$ for all positive integers d relatively prime to p.

In the rest of the paper, we provide explicit examples of the Ekedahl–Oort structure of $\mathcal{C}_d$ and the four associated invariants under various conditions on d and p. In Section 8, we separate out the case $p = 2$. In Section 9, we determine the a-number of $\mathcal{C}_d$ for all d relatively prime to p. In Sections 10 and 11, we analyze the cases $d = p^\ell - 1$ and $d = p^\ell + 1$, for any natural number ℓ. We call $d = p^\ell - 1$ the "encompassing case"; it is in some sense the general case because for every d', the group scheme $\mathrm{Jac}(C_{d'})[p]$ is a direct factor of $\mathrm{Jac}(C_d)[p]$ where $d = p^\ell - 1$ for some ℓ.

Acknowledgements. Author RP was partially supported by NSF grant DMS-1901819, and author DU was partially supported by Simons Foundation grants 359573 and 713699. We would like to thank the referee for a thoughtful and very fast report.

2. Groups and modules

In this section, we review certain categories of group schemes and their Dieudonné modules.

2.1. Group schemes of p-power order and their Dieudonné modules. Our general reference for the assertions in this section is [Fon77].

Let $W(k)$ denote the Witt vectors over k. Write σ for the absolute Frobenius of k, and extend it to $W(k)$ by $\sigma(a_0, a_1, \dots) = (a_0^p, a_1^p, \dots)$. Define the *Dieudonné ring* $\mathbb{D} = W(k)\{F, V\}$ as the $W(k)$-algebra generated by symbols F and V with relations

$$FV = VF = p,\ F\alpha = \sigma(\alpha)F,\ \text{and}\ \alpha V = V\sigma(\alpha)\ \text{for}\ \alpha \in W(k). \tag{2.1}$$

Let $\mathbb{D}_k = \mathbb{D}/p\mathbb{D} \cong k\{F, V\}$.

Let G be a finite commutative group scheme of order p^ℓ over k. Let $M(G)$ be the (contravariant) Dieudonné module of G. This is a $W(k)$-module of length ℓ with semi-linear operators F and V.

Let G^D be the Cartier dual of G. For M a $\mathbb{D}$-module of finite length over $W(k)$, let M^* be its dual module. A basic result of Dieudonné theory is that $M(G^D) \cong M(G)^*$.

2.2. BT_1 group schemes and BT_1 modules. By definition, a BT_1 *group scheme* over k is a finite commutative group scheme G that is killed by p and that has the properties

$$\operatorname{Ker}(F : G \to G^{(p)}) = \operatorname{Im}(V : G^{(p)} \to G)$$

and

$$\operatorname{Im}(F : G \to G^{(p)}) = \operatorname{Ker}(V : G^{(p)} \to G).$$

The notation BT_1 is an abbreviation of "Barsotti–Tate of level 1" reflecting the fact [Ill85, Prop. 1.7] that BT_1 group schemes are precisely those which occur as the kernel of p on a Barsotti–Tate (=p-divisible) group.

By definition, a BT_1 *module* over k is a $\mathbb{D}_k$-module M of finite dimension over k such that

$$\operatorname{Ker}(F : M \to M) = \operatorname{Im}(V : M \to M)$$

and

$$\operatorname{Im}(F : M \to M) = \operatorname{Ker}(V : M \to M).$$

(Oort also calls these DM_1 modules.) Clearly, a $\mathbb{D}_k$-module M is a BT_1 module if and only if it is the Dieudonné module of a BT_1 group scheme over k.

The group schemes $\mathbb{Z}/p\mathbb{Z}$, μ_p, and $G_{1,1}$[1] are BT_1 group schemes. On the other hand, α_p is not, since $\operatorname{Ker} F = M(\alpha_p) \neq 0 = \operatorname{Im} V$.

A BT_1 group scheme G is *self-dual* if there exists an isomorphism $G \cong G^D$. Similarly, a BT_1 module M is *self-dual* if $M \cong M^*$. Clearly, G is self-dual if and only if $M(G)$ is self-dual.

One may ask that a duality $\phi : G \to G^D$ be skew, meaning that $\phi^D : G \cong (G^D)^D \to G^D$ satisfies $\phi^D = -\phi$. This is equivalent to any of the following three conditions:

- the bilinear pairing $G \times G \to \mathbb{G}_m$ induced by ϕ is skewsymmetric;
- the duality $M(\phi) : M(G)^* \to M(G)$ is skew, meaning that $M(\phi)^* = -M(\phi)$;
- the induced pairing $M(G)^* \times M(G)^* \to k$ is skewsymmetric.

Interestingly, when $p = 2$, there exist BT_1 group schemes G with an *alternating* pairing ($\langle x, x\rangle = 0$ for all x) such that the induced pairing on $M(G)$ is skewsymmetric but not alternating.

For this reason, one defines a *polarized* BT_1 *module* over k as a BT_1 module over k with a non-degenerate, alternating pairing, and one defines a *polarized* BT_1 *group scheme* over k as a BT_1 group scheme G over k with a pairing that induces a non-degenerate, alternating pairing on $M(G)$. Corollary 4.2 says that every self-dual BT_1 module admits a polarization which is unique up to isomorphism.

[1] the kernel of p on a supersingular elliptic curve

If A is a principally polarized abelian variety of dimension g over k , its p-torsion subscheme $A[p]$ is naturally a polarized BT_1 group scheme of order p^{2g}.

3. Review of classifications of BT_1 group schemes

In this section, we review bijections between isomorphism classes of BT_1 modules over k and three other classes of objects of combinatorial nature. More precisely, following Kraft [Kra][2] Ekedahl, and Oort [Oor01], we will construct a diagram of isomorphism classes:

$$\begin{array}{ccc} BT_1 \text{ modules} & \xrightarrow{\sim} & \text{canonical types} \\ \Big\uparrow{\scriptstyle\sim} & & \Big\downarrow{\scriptstyle\sim} \\ \begin{array}{c}\text{multisets of (primitive)} \\ \text{cyclic words on } \{f,v\}\end{array} & \longleftrightarrow & \begin{array}{c}\text{(admissible) permutations} \\ \text{of } S = S_f \cup S_v.\end{array} \end{array} \tag{3.1}$$

The top horizontal map is the Ekedahl–Oort classification of BT_1 modules and the left vertical map is the Kraft classification. While some of the material in this section is known, there are significant reasons to cover it, and we take the opportunity to correct a few minor imprecisions in the literature. First, it is helpful to have a self-contained short description of this material. Second, we need a precise dictionary between the classification on the lower right of the diagram, given in terms of permutations, and the others. The permutation classification is not as well known and is particularly well suited to studying the p-torsion group schemes of quotients of Fermat curves. Third, the work of Oort uses covariant Dieudonné theory, but the contravariant theory is more convenient for studying Fermat curves.

There are other classifications of BT_1 modules, one due to Moonen [Moo01], involving cosets of Weyl groups; and another due to van der Geer [vdG99, §6] in terms of Young diagrams and partitions. We will not need this material, so we omit any further discussion.

3.1. Words and permutations. In this section, we describe the bijection on the bottom row of Diagram (3.1). Let $\mathcal{W}$ be the monoid of words w on the two-letter alphabet $\{f, v\}$, and write 1 for the empty word. By convention, the first (resp. last) letter of w is its leftmost (resp. rightmost) letter. The complement w^c of w is the word obtained by exchanging f and v at every letter.

For a positive integer λ, write $\mathcal{W}_\lambda$ for the words of length λ. Endow $\mathcal{W}_\lambda$ with the lexicographic ordering with $f < v$. If $w \in \mathcal{W}_\lambda$, we write $w = u_{\lambda-1} \cdots u_0$ where $u_i \in \{f, v\}$ for $0 \leq i \leq \lambda - 1$. Define an action of the group $\mathbb{Z}$ on $\mathcal{W}$ by requiring that $1 \in \mathbb{Z}$ map $w = u_{\lambda-1} \cdots u_0$ to $u_0 u_{\lambda-1} \cdots u_1$. If w and w' are in the same orbit of this action, we say w' is a *rotation* of w.

[2] Kraft's manuscript is unpublished and, as far as we know, not available online. However, the results from Kraft that we use are reestablished in [Oor01].

The orbit $\overline{w}$ of w under the action of $\mathbb{Z}$ is called a *cyclic word*. Write $\overline{\mathcal{W}}$ for the set of cyclic words.

A word w is *primitive* if w is not of the from $(w')^e$ for some word w' and some integer $e > 1$. If w has length $\lambda > 0$, it is primitive if and only if the subgroup of $\mathbb{Z}$ fixing w is exactly $\lambda\mathbb{Z}$. Write $\mathcal{W}'$ for the set of primitive words and $\overline{\mathcal{W}}'$ for the set of primitive cyclic words. At the level of multisets, one can define a retraction of $\overline{\mathcal{W}}' \subset \overline{\mathcal{W}}$ by sending the class of a word $w = (w')^e$ where w' is primitive to the class of w' with multiplicity e.

Consider a finite set S written as the disjoint union $S = S_f \cup S_v$ of two subsets and a permutation $\pi : S \to S$. Two such collections of data $(S = S_f \cup S_v, \pi)$ and $(S' = S'_f \cup S'_v, \pi')$ are isomorphic if there is a bijection $\iota : S \to S'$ such that $\iota(S_f) = S'_f$, $\iota(S_v) = S'_v$, and $\iota\pi = \pi'\iota$.

Given $(S = S_f \cup S_v, \pi)$, there is an associated multiset of cyclic words on $\{f, v\}$ defined as follows. For $a \in S$ with orbit of size λ, define the word $w_a = u_{\lambda-1} \cdots u_0$ where

$$u_j = f \text{ if } \pi^j(a) \in S_f, \text{ and } u_j = v \text{ if } \pi^j(a) \in S_v.$$

Then $\overline{w}_a$ depends only on the orbit of a. This gives a well-defined map from orbits of π to cyclic words, i.e., elements of $\overline{\mathcal{W}}$. Taking the union over orbits, we can associate to $(S = S_f \cup S_v, \pi)$ a multiset of cyclic words. If S and S' are isomorphic, then they yield the same multiset.

Conversely, given a multiset of cyclic words, let S be the set of all words representing them (repeated to account for multiplicities), let S_f be the subset of those words ending with f, let S_v be the subset of those words ending with v, and let π be defined by the action of $1 \in \mathbb{Z}$ as above.

The data $(S = S_f \cup S_v, \pi)$ is *admissible* if the associated words w_a for $a \in S$ are primitive.

3.2. Cyclic words to BT_1 modules. Following Kraft [Kra], we attach a BT_1 module to a multiset of primitive cyclic words. This defines the left vertical arrow of Diagram (3.1).

3.2.1. Construction. Suppose that $w \in \mathcal{W}'$ is a primitive word, say $w = u_{\lambda-1} \cdots u_0$ with $u_j \in \{f, v\}$. Let $M(w)$ be the k-vector space with basis e_j with $j \in \mathbb{Z}/\lambda\mathbb{Z}$ and define a p-linear map $F : M(w) \to M(w)$ and a p^{-1}-linear map $V : M(w) \to M(w)$ by setting

$$F(e_j) = \begin{cases} e_{j+1} & \text{if } u_j = f, \\ 0 & \text{if } u_j = v, \end{cases} \qquad \text{and} \qquad V(e_{j+1}) = \begin{cases} e_j & \text{if } u_j = v, \\ 0 & \text{if } u_j = f. \end{cases}$$

(Note that $F(e_j) \neq 0$ exactly when the last letter of the j-th rotation of w is f, and $V(e_{j+1}) \neq 0$ exactly when the last letter of the j-th rotation of w is v.) This construction yields a BT_1 module which up to isomorphism only depends on the primitive cyclic word $\overline{w}$ associated to w.

Kraft proves that $M(w)$ is indecomposable and that every indecomposable BT_1 module is isomorphic to one of the form $M(w)$ for a unique primitive cyclic word $\overline{w}$. Thus every BT_1 module M is isomorphic to a direct sum $\oplus M(w_i)$ where $\overline{w}_i$ runs through a uniquely determined multiset of primitive cyclic words.

If w is a word that is not necessarily primitive, the formulas above define a BT_1 module. If $w = (w')^e$, Kraft also proves that $M(w) \cong M(w')^e$.

It is clear that $M(f) = M(\mathbb{Z}/p\mathbb{Z})$, $M(v) = M(\mu_p)$, and $M(fv)$ is the Dieudonné module of the kernel of p on a supersingular elliptic curve. More generally, if w has length > 1 and is primitive, then $M(w)$ is the Dieudonné module of a unipotent, connected BT_1 group scheme.

3.2.2. Generators and relations. Let w be a primitive word with associated BT_1 module $M(w)$. It will be convenient to have a presentation of $M(w)$ by generators and relations. Clearly, $M(f) = \mathbb{D}_k/(F-1, V)$ and $M(v) = \mathbb{D}_k/(F, V-1)$.

Now suppose w has length > 1. Then, after rotating w if necessary, we may assume its last letter is f and its first letter is v. (Both letters appear because w is primitive, so in particular is not f^m nor v^n.) We then write w in exponential notation as

$$w = v^{n_r} f^{m_r} \cdots v^{n_1} f^{m_1},$$

for some positive integers $r, m_1, \ldots, m_r, n_1, \ldots, n_r$.

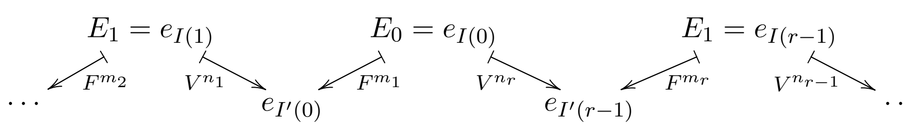
Lemma 3.1. *The BT_1 module $M(w)$ admits generators E_i and relations $F^{m_i} E_{i-1} = V^{n_i} E_i$ for $i \in \mathbb{Z}/r\mathbb{Z}$.*

Proof. Indeed, for $i = 0, \ldots, r-1$, let $I(i) = \sum_{j=1}^{i} (m_j + n_j)$, let $I'(i) = I(i) + m_{i+1}$, and let $E_i = e_{I(i)}$. The E_i generate $M(w)$ as a $\mathbb{D}_k$-module because

$$\text{if } I(i) \le j \le I'(i), \text{ then } e_j = F^{j-I(i)} E_i,$$
$$\text{and if } I'(i) \le j \le I(i+1), \text{ then } e_j = V^{j-I'(i)} E_{i+1},$$

and there are relations $F^{m_i} E_{i-1} = e_{I'(i-1)} = V^{n_i} E_i$. □

The following diagram illustrates this presentation of $M(w)$:



3.3. BT_1 modules to canonical types. Following Oort [Oor01], we explain how to describe the isomorphism class of a BT_1 module in terms of certain combinatorial data. This defines the top horizontal arrow in Diagram (3.1). Readers are invited to work through the example in Section 3.3.2 while reading this section.

Warning: Many of our formulas differ from those in [Oor01] for two reasons: first, we use the contravariant Dieudonné theory, whereas Oort uses the covariant theory; second, Oort studies a filtration defined by F^{-1} and V, whereas we use F and V^{-1}. The two approaches are equivalent (and exchanged under duality), but the latter is more convenient for studying Fermat curves.

3.3.1. The canonical filtration. Recall that $\mathcal{W}$ denotes the monoid of words on $\{f, v\}$. Let M be a BT_1 module, and define a left action of $\mathcal{W}$ on the set of k-subspaces of M by requiring that

$$fN := F(N) \text{ and } vN := V^{-1}(N).$$

In other words, f sends a subspace N to its image under F and v sends N to its inverse image under V. Note that if $N_1 \subset N_2$, then $fN_1 \subset fN_2$ and $vN_1 \subset vN_2$. If N is a $\mathbb{D}_k$-module, so are fN and vN, and $fN \subset N \subset vN$. Also note that $fM = \operatorname{Im} F = \operatorname{Ker} V = v0$.

Let M be a BT_1 module. An *admissible filtration* on M is a filtration by $\mathbb{D}_k$-modules

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_s = M, \tag{3.1}$$

such that for all i, there exist indices $\phi(i)$ and $\nu(i)$ such that $fM_i = M_{\phi(i)}$ and $vM_i = M_{\nu(i)}$.

Definition 3.2. The *canonical filtration* on M is the coarsest admissible filtration on M. If Equation (3.1) is the canonical filtration, the *blocks* of M are $B_i = M_{i+1}/M_i$ for $0 \le i \le s-1$.

The canonical filtration of M is constructed by enumerating all subspaces of M of the form wM and indexing them in order of containment. Define s to be the number of steps in the filtration and r to be the integer such that $M_r = fM = v0$. Define functions ϕ, ν, and ρ by

$$\phi : \{0, \dots, s\} \to \{0, \dots, r\}, \quad fM_i = M_{\phi(i)},$$
$$\nu : \{0, \dots, s\} \to \{r, \dots, s\}, \quad vM_i = M_{\nu(i)},$$

and

$$\rho : \{0, \dots, s\} \to \mathbb{Z}, \quad \rho(i) = \dim_k M_i.$$

This data has the following properties.

Proposition-Definition 3.3. *The data (r, s, ϕ, ν, ρ) associated to the canonical filtration of M is a* canonical type*, i.e., $s > 0$, $0 \le r \le s$, and the functions ϕ, ν, and ρ have the following properties:*

1. *ϕ and ν are monotone nondecreasing and surjective;*
2. *ρ is strictly increasing with $\rho(0) = 0$;*
3. *$\nu(i+1) > \nu(i)$ if and only if $\phi(i+1) = \phi(i)$;*
4. *if the equivalent conditions in (3) are true, then $\rho(i+1) - \rho(i) = \rho(\nu(i)+1) - \rho(\nu(i))$, while if not, then $\rho(i+1) - \rho(i) = \rho(\phi(i)+1) - \rho(\phi(i))$;*
5. *and every integer in $\{1, \dots, s\}$ can be obtained by repeatedly applying ϕ and ν to s.*

If the data (r, s, ϕ, ν, ρ) comes from the canonical filtration of a BT_1 module, then it is clear from the definitions that $0 \leq r \leq s$, with $s > 0$, and that properties (1), (2), and (5) hold. Oort proves that properties (3) and (4) hold in [Oor01, §2].

The properties imply that $\nu(i+1) - \nu(i)$ and $\phi(i+1) - \phi(i)$ are either 0 or 1, that exactly one of them is 1, and that $\nu(i) + \phi(i) = r + i$. The next lemma will be used in later sections.

Lemma 3.4. [Oor01, Lemma 2.4] *Let* (3.1) *denote the canonical filtration of M and let $B_i = M_{i+1}/M_i$ for $0 \leq i \leq s-1$. If $\phi(i+1) > \phi(i)$ then F induces a p-linear isomorphism $B_i \tilde{\to} B_{\phi(i)}$, and if $\nu(i+1) > \nu(i)$, then V^{-1} induces a p-linear isomorphism $B_i \tilde{\to} B_{\nu(i)}$.*

The key assertion is that the canonical type of M determines M up to isomorphism:

Proposition 3.5. *If the canonical types of two BT_1 modules M, M' are equal, then $M \cong M'$.*

Oort proves a related result [Oor01, Thm. 9.4] with quasi-polarizations (pairings) which is more involved and only applies to self-dual BT_1 modules. Moonen proves the result stated here [Moo01, §4] in the more general context where the module M also has endomorphisms by a semi-simple $\mathbb{F}_p$-algebra D; taking $D = \mathbb{F}_p$ yields Proposition 3.5.

Remark 3.6. Let $\mu : \{0, \ldots, s-1\} \to \mathbb{Z}$ be defined by $\mu(i) = \rho(i+1) - \rho(i)$. Equivalently, $\mu(i) = \dim_k(B_i)$. Property (2) says μ takes positive values, and property (4) says if $\nu(i+1) > \nu(i)$, then $\mu(i) = \mu(\nu(i))$ and if $\phi(i+1) > \phi(i)$, then $\mu(i) = \mu(\phi(i))$.

Remark 3.7. Oort defines a canonical type to be data as above satisfying properties (1)–(4), i.e., he omits (5), and he states [Oor01, Remark 2.8] that every canonical type comes from a BT_1 module. With this definition, it is true that every canonical type comes from an admissible filtration on a BT_1 module, but not necessarily from the *canonical* filtration. Here is a counterexample: Let $r = 0$, $s = 2$ and $\phi(i) = 0$, $\nu(i) = i$ and $\rho(i) = i$ for $i = 0, 1, 2$. This data comes from a filtration on $N = M((\mu_2)^2)$ and it satisfies properties (1)–(4), but not (5). The canonical type of N has $r = 0$, $s = 1$, $\phi(i) = 0$, $\nu(i) = i$ for $i = 0, 1$, and $\rho(0) = 0$, $\rho(1) = 2$.

3.3.2. An example. Let M be the k-vector space with basis $e_1, \ldots, e_7$ and action of F, V given by

e	e_1	e_2	e_3	e_4	e_5	e_6	e_7
$F(e)$	0	0	0	e_1	e_2	0	e_3
$V(e)$	0	0	0	e_1	e_2	e_3	e_6

.

Using $\langle \dots \rangle$ to denote the span of a set of vectors, the canonical filtration of M is

$$M_0 = 0 \subset M_1 = \langle e_1, e_2 \rangle \subset M_2 = \langle e_1, e_2, e_3 \rangle \subset M_3 = \langle e_1, e_2, e_3, e_4, e_5 \rangle \\ \subset M_4 = \langle e_1, e_2, e_3, e_4, e_5, e_6 \rangle \subset M_5 = \langle e_1, e_2, e_3, e_4, e_5, e_6, e_7 \rangle = M.$$

The canonical type is given by $s = 5$, $r = 2$, and the functions ϕ, ν, ρ below:

i	0	1	2	3	4	5
$\phi(i)$	0	0	0	1	1	2
$\nu(i)$	2	3	4	4	5	5
$\rho(i)$	0	2	3	5	6	7

.

3.4. Canonical types to permutations. Following [Oor01, Section 2], we explain how to use a canonical type to define a partitioned set $S = S_f \cup S_v$ with permutation $\pi : S \to S$, thus defining the right vertical arrow of Diagram (3.1). These results cast considerable light on the structure of BT_1 modules, but they will not be used explicitly in the rest of the paper.

Let (r, s, ϕ, ν, ρ) be as in Definition 3.3, and let $\Gamma = \{0, \dots, s-1\}$. Define $\Pi : \Gamma \to \Gamma$ by:

$$\Pi(i) = \begin{cases} \phi(i) & \text{if } \phi(i+1) > \phi(i), \\ \nu(i) & \text{if } \nu(i+1) > \nu(i). \end{cases}$$

Property (3) of Definition 3.3 shows that Π is well defined. Property (1) implies that Π is injective and thus bijective. By Property (4), $\mu(i) = \rho(i+1) - \rho(i)$ is constant on the orbits of Π.

We partition Γ as a disjoint union $\Gamma_f \cup \Gamma_v$ where $i \in \Gamma_f$ if and only if $\pi(i) = \phi(i)$. Equivalently,

$$\Gamma_f = \{ i \in \Gamma \mid \phi(i+1) > \phi(i) \} \quad \text{and} \quad \Gamma_v = \{ i \in \Gamma \mid \nu(i+1) > \nu(i) \}.$$

Then (r, s, ϕ, ν, ρ) is determined by the data $\Gamma = \Gamma_f \cup \Gamma_v$, $\Pi : \Gamma \to \Gamma$, and $\mu : \Gamma \to \mathbb{Z}$.

3.4.1. Example 3.3.2 continued. In this case, the permutation Π of $\Gamma = \{0, 1, 2, 3, 4\}$ is $(0, 2)(1, 3, 4)$, the partition is given by $\Gamma_f = \{2, 4\}$ and $\Gamma_v = \{0, 1, 3\}$, and the associated words are

$$w_0 = fv, \; w_1 = fvv, \; w_2 = vf, \; w_3 = vfv, \text{ and } w_4 = vvf.$$

Note that $\mu(0) = \mu(2) = 2$ and $\mu(1) = \mu(3) = \mu(4)$, so μ is constant on the orbits of Π.

To complete the definition of the right vertical arrow of Diagram (3.1), we use μ as a set of "multiplicities" to expand Γ into S. More precisely, define

$$S := \{ e_{i,j} \mid i \in \Gamma, 1 \le j \le \mu(i) \}$$

with partition

$$S_f = \{ e_{i,j} \in S \mid i \in \Gamma_f \} \quad \text{and} \quad S_v = \{ e_{i,j} \in S \mid i \in \Gamma_v \}$$

and permutation $\pi : S \to S$ with $\pi(e_{i,j}) := e_{\Pi(i),j}$.

Lemma 3.8. *The data* $(S = S_f \cup S_v, \pi)$ *is an* admissible *permutation.*

Proof. The set of cyclic words associated to $(S = S_f \cup S_v, \pi)$ is the same as the set of cyclic words associated to $(\Gamma = \Gamma_f \cup \Gamma_v, \Pi)$. We need to show that these words are primitive. If $w = w_i$ for $i \in \Gamma$, then $w_{\Pi^j(i)}$ is the j-th cyclic rotation of w_i. Thus to show that the w_i are all primitive, it suffices to show that they are distinct.

To that end, define a left action of the monoid $\mathcal{W}$ on the set $\{0, \dots, s\}$ by requiring that $f(i) = \phi(i)$ and $v(i) = \nu(i)$. If $i \in \Gamma$, and if w_i is the word associated to i, then w_i fixes i and $i+1$. This is a manifestation in the canonical type of the isomorphisms from Lemma 3.4:

$$B_i \xrightarrow{\sim} B_{\Pi(i)} \xrightarrow{\sim} B_{\Pi^2(i)} \xrightarrow{\sim} \cdots \xrightarrow{\sim} B_i.$$

Now assume that $i, j \in \Gamma$, $i < j$, and $w_i = w_j = w$. We will deduce a contradiction of property (5) in Definition 3.3. Since ϕ and ν are nondecreasing, for all $n > 0$ we have

$$w^n(s) \geq i+1 > i \geq w^n(0) \quad \text{and} \quad w^n(s) \geq j+1 > j \geq w^n(0),$$

so $w^n(s) \geq j+1$ and $i \geq w^n(0)$ for all $n > 0$.

Choose some i' with $i < i' \leq j$. By property (5) of Definition 3.3, there is a word w' with $w'(s) = i'$. Choose $n > 0$ large enough that w^n is at least as long as w', and then replace w' with $w'v^m$ where m is chosen so w^n and w' have the same length. Since $v(s) = \nu(s) = s$, we still have $w'(s) = i'$. If $w' \geq w^n$ (in the lexicographic order from Section 3.1), then $i' = w'(s) \geq w^n(s) \geq j+1$, a contradiction; and if $w' < w^n$, then $i' = w'(s) \leq w^n(0) \leq i$, again a contradiction. We conclude that there can be no $i < j$ with $w_i = w_j$, and thus π is admissible. $\square$

Remark 3.9. A more thorough analysis along these lines shows that if M is a BT_1 module, then there are finitely many primitive words w_i such that $w_i^n M \supsetneq w_i^n 0$ for all $n > 1$. Enumerate these as $w_0, \dots, w_{s-1}$ and choose integers n_i so that $w_i^n M = w_i^{n_i} M$ and $w_i^n 0 = w_i^{n_i} 0$ for all $n \geq n_i$, and so that the lengths of the $w_i^{n_i}$ are all the same. Define $\tilde{w}_i = w_i^{n_i}$. Reorder the w_i so that

$$\tilde{w}_0 < \tilde{w}_1 < \cdots < \tilde{w}_{s-1}.$$

(Numbering the $\tilde{\omega}_i$ from $i = 0$ turns out to be most convenient; see the proof of Lemma 9.6.) Let $\tilde{w}_{-1} M = 0$. Then the w_i are distinct, the canonical filtration of M is

$$0 \subsetneq \tilde{w}_0 M \subsetneq \cdots \subsetneq \tilde{w}_{s-1} M = M,$$

and the primitive words associated to M are precisely the w_i, with the multiplicity of w_i being

$$\mu(i) = \dim_k(\tilde{w}_i M / \tilde{w}_{i-1} M).$$

3.5. Words to canonical types. In this section, we describe the map from multisets of (not necessarily primitive) cyclic words to canonical type. This will be used in Sections 5 and 7.

For $1 \leq i \leq n$, let $\overline{w}_i$ be cyclic words with multiplicities m_i. Let $M(\overline{w}_i)$ be the Kraft module discussed in Section 3.2. Our goal is to describe the canonical type of the BT_1 module

$$M = \bigoplus_{i=1}^{n} M(\overline{w}_i)^{m_i}.$$

Let λ_i be the length of $\overline{w}_i$ and choose a representative $w_i = u_{i,\lambda_i-1} \cdots u_{i,0}$ of $\overline{w}_i$ with $u_{i,j} \in \{f, v\}$. The k-vector space underlying M has basis $e_{i,j,k}$ where $1 \leq i \leq n$, $j \in \mathbb{Z}/\lambda_i\mathbb{Z}$, and $1 \leq k \leq m_i$. Its $\mathbb{D}_k$-module structure is given by

$$F(e_{i,j,k}) = \begin{cases} e_{i,j+1,k} & \text{if } u_{i,j} = f, \\ 0 & \text{if } u_{i,j} = v, \end{cases}$$

and

$$V(e_{i,j+1,k}) = \begin{cases} e_{i,j,k} & \text{if } u_{i,j} = v, \\ 0 & \text{if } u_{i,j} = f. \end{cases}$$

Let $w_{i,j} = u_{i,j-1} \cdots u_{i,0} u_{i,\lambda_i} \cdots u_{i,j}$ be the j-th rotation of w_i. Let $\ell = \mathrm{LCM}(\lambda_i)_{i=1..n}$ and set $\tilde{w}_{i,j} = w_{i,j}^{\ell/\lambda_i}$. Thus each $\tilde{w}_{i,j}$ has length ℓ and we may compare them in lexicographic order.

Let Σ be the multiset obtained by including each $\tilde{w}_{i,j}$ with multiplicity m_i. (The $\tilde{w}_{i,j}$ need not be distinct, and if there are repetitions, one should add multiplicities.) Now relabel the distinct elements of Σ as ω_t for $0 \leq t \leq s-1$ and ordered so that $\omega_0 < \omega_1 < \cdots < \omega_{s-1}$. Let τ be the function such that $\tau(i,j) = t$ if and only if $\tilde{w}_{i,j} = \omega_t$. Let $\mu(t)$ be the multiplicity of ω_t in Σ.

For $1 \leq t \leq s$, let M_t be the k-subspace of M spanned by those $e_{i,j,k}$ with $\tau(i,j) \leq t-1$. We claim that the canonical filtration of M is

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_s = M.$$

Indeed, it is easy to see that if ω_t ends with f and $\omega_{t'}$ is the first rotation of ω_t, then F induces a p-linear isomorphism $M_{t+1}/M_t \tilde{\to} M_{t'+1}/M_{t'}$. On the other hand, if ω_t ends with v, then V^{-1} induces a p-linear isomorphism $M_{t+1}/M_t \tilde{\to} M_{t'+1}/M_{t'}$. Thus the displayed filtration is an admissible filtration. Via the action of $\mathcal{W}$ on M, the word ω_t induces a semi-linear automorphism of M_{t+1}/M_t, while a power of ω_t induces the zero map of $M_{t'+1}/M_{t'}$ if $t \neq t'$. It follows that $\omega_t^n M = M_{t+1}$ for large enough n, so this is the coarsest filtration, thus the canonical filtration.

The dimension of the block $B_t = M_{t+1}/M_t$ equals $\mu(\omega_t)$, the multiplicity of ω_t in Σ.

It remains to record the values of r and the functions ϕ, ν, and ρ associated to M:

- $r = \#\{t \mid 0 \le t < s,\ \omega_t \text{ ends with } f\}$;
- $\phi(i) = \#\{t \mid 0 \le t < i,\ \omega_t \text{ ends with } f\}$;
- $\nu(i) = r + \#\{t \mid 1 \le t < i,\ \omega_t \text{ ends with } v\}$; and
- $\rho(i) = \sum_{t=0}^{i-1} \mu(t)$.

3.5.1. Example. Let $\overline{w}_1 = \overline{fv}$, $w_2 = \overline{fvfv}$, and $m_1 = m_2 = 1$. Taking $n_1 = 2$ and $n_2 = 1$, one finds that Σ contains $\omega_0 = fvfv$ and $\omega_1 = vfvf$, each with multiplicity 3. The function τ is

$$\tau(1,0) = \tau(2,0) = \tau(2,2) = 0 \quad \text{and} \quad \tau(1,1) = \tau(2,1) = \tau(2,1) = 1,$$

and $\mu(0) = \mu(1) = 3$. Thus $s = 2$, $r = 1$, and the functions ϕ, ν, and ρ are given by

i	0	1	2
$\phi(i)$	0	0	1
$\nu(i)$	1	2	2
$\rho(i)$	0	3	6

4. Duality and E–O structures

4.1. Duality of BT_1 modules. We record how duality of BT_1 modules interacts with the objects in Diagram (3.1). All the assertions in this section will be left to the reader.

For a BT_1 module M, let M^* is its dual. If $N \subset M$ is a k-subspace, then

$$F\left(N^{\perp}\right) = \left(V^{-1}N\right)^{\perp} \quad \text{and} \quad V^{-1}\left(N^{\perp}\right) = (FN)^{\perp}.$$

Let

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_s = M$$

be the canonical filtration of M; setting $M_i^* = (M_{s-i})^{\perp}$, then the canonical filtration of M^* is

$$0 = M_0^* \subsetneq M_1^* \subsetneq \cdots \subsetneq M_s^* = M^*.$$

If the canonical data attached to M is (r, s, ϕ, ν, ρ), and the canonical data attached to M^* is $(r^*, s^*, \phi^*, \nu^*, \rho^*)$, then $s^* = s$, $r^* = s - r$, and for $0 \le i \le s$,

$$\phi^*(i) = s - \nu(s-i),\ \nu^*(i) = s - \phi(s-i),\ \text{and } \rho^*(i) = \rho(s) - \rho(s-i).$$

It follows that M is self-dual if and only if the associated canonical data satisfies $s = 2r$,

$$\phi(i) + \nu(s-i) = s,\ \text{and } \rho(i) + \rho(s-i) = \rho(s). \tag{4.1}$$

The relationship between the partitioned set with permutation associated to M and to M^* is $S^* = S$, $S_f^* = S_v$, $S_v^* = S_f$, and $\pi^* = \pi$. It follows that M is self-dual if and only if there exists a bijection $\iota : S \tilde{\to} S$ which satisfies $\iota(S_f) = S_v$ and $\pi \circ \iota = \iota \circ \pi$.

If w is a primitive word on $\{f, v\}$, define w^c to be the word obtained by exchanging f and v. This operation descends to a well-defined involution on cyclic words and $M(w)^* \cong M(w^c)$. It follows that M is self-dual if and only if the associated multiset of cyclic primitive words consists of self-dual words ($\overline{w}^c = \overline{w}$) and pairs of dual words ($\{\overline{w}, \overline{w}^c\}$).

4.2. Ekedahl–Oort classification of polarized BT_1 modules. Clearly, a polarized BT_1 module is self-dual. Conversely, as we will see below (Corollary 4.2), any self-dual BT_1 module can be given a polarization. In this section, we review the Ekedahl–Oort classification [Oor01] of polarized BT_1 modules.

4.2.1. Elementary sequences. Elementary sequences are a convenient repackaging of the data of a self-dual canonical type (r, s, ϕ, ν, ρ). Using Equation (4.1), the restrictions of ϕ and ρ to $\{0, \ldots, r\}$ determine the rest of the data. An *elementary sequence* of length g is a sequence $\Psi = [\psi_1, \ldots, \psi_g]$ of integers with $\psi_{i-1} \le \psi_i \le \psi_{i-1} + 1$ for $i = 1, \ldots, g$ and $\psi_0 = 0$. The set of elementary sequences of length g has cardinality 2^g.

Given (r, s, ϕ, ν, ρ), define an elementary sequence as follows. Let $g = \rho(r)$. Set $\psi_0 = 0$. For each $1 \le j \le g$, let i be the unique integer $0 < i \le r$ such that $\rho(i-1) < j \le \rho(i)$. Define

$$\psi_j = \begin{cases} \psi_{j-1} & \text{if } \phi(i) = \phi(i-1), \\ \psi_{j-1} + 1 & \text{if } \phi(i) > \phi(i-1). \end{cases}$$

(Put more vividly, the sequence ψ_j increases for $\mu(i-1)$ steps if $\phi(i) > \phi(i-1)$ and it stays constant for $\mu(i-1)$ steps if $\phi(i) = \phi(i-1)$.)

We leave it as an exercise for the reader to check that, given an elementary sequence, there is a unique self-dual canonical type giving rise to it by this construction.

Elementary sequences can be obtained directly from a self-dual BT_1 module as follows: The canonical filtration can be refined into a "final filtration," i.e., a filtration

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{2g} = M$$

respected by F and V^{-1} and such that $\dim_k(M_i) = i$. Then Ψ is defined by $\psi_i = \dim_k(FM_i)$.

Theorem 4.1. [Oor01, Thm. 9.4] *Every elementary sequence of length g arises from a polarized BT_1 module of dimension $2g$, and two polarized BT_1 modules over k with the same elementary sequences are isomorphic. More precisely, there is an isomorphism of BT_1 modules which respects the alternating pairings.* (*This isomorphism is not unique in general.*)

The elementary sequence attached to a BT_1 module is also called its *Ekedahl–Oort structure.*

Corollary 4.2. *Every self-dual BT_1 module admits a polarization, i.e., a non-degenerate* alternating *pairing, and this pairing is unique up to* (*non-unique*) *isomorphism.*

Proof. If M is a self-dual BT_1 module, construct its canonical type, and its elementary sequence Ψ as in Section 4.2.1. Theorem 4.1 furnishes a polarized BT_1 module with the same underlying BT_1 module, and this proves the existence of a polarization. For uniqueness, note that the construction of Ψ does not depend on the pairing. So, given two alternating pairings on M, Theorem 4.1 shows there is a (not necessarily unique) automorphism intertwining the pairings. □

5. Homomorphisms

The Kraft description of BT_1 modules is well adapted to computing homomorphisms. We work out three important examples in this section.

5.1. Homs from $\mathbb{Z}/p\mathbb{Z}$ or μ_p.

Definition 5.1. If G is a BT_1 group scheme, the *p-rank* of G is the largest integer f such that there is an injection $(\mathbb{Z}/p\mathbb{Z})^f \hookrightarrow G$. Alternatively, f is the dimension of the largest quotient space of $M(G)$ on which Frobenius acts bijectively.

Lemma 5.2. *If G is a BT_1 group scheme, the p-rank of G is equal to the multiplicity of the word f in the multiset of primitive words corresponding to $M(G)$. Similarly, the largest f such that μ_p^f embeds in $M(G)$ is the multiplicity of the word v.*

Proof. From the presentation in terms of generators and relations, we see that if w is a primitive word other than f, then there is no non-zero homomorphism from $\mathbb{Z}/p\mathbb{Z} = M(f)$ to $M(w)$. It follows that if $M(G)$ is given in the Kraft classification by a multiset of primitive cyclic words, the p-rank is the multiplicity of the word f. The assertion for μ_p is proved analogously. □

5.2. Homs from α_p. Let G be a finite group scheme over k killed by p. Define the *foot* (or *socle*) of G to be the largest semisimple subgroup of G. The simple objects in the category of finite group schemes over k killed by p are $\mathbb{Z}/p\mathbb{Z}$, μ_p, and α_p. Thus the foot of G is a direct sum of these (with multiplicity). If G is connected and unipotent, then its foot is of the form α_p^ℓ for some positive integer ℓ. Note that $M(\alpha_p) = \mathbb{D}_k/(F, V)$.

Similarly, if M is a $\mathbb{D}_k$-module of finite length, the *head* (or *co-socle*) of M is its largest semisimple quotient. We write $\mathcal{H}(M)$ for the head of M. If M is a $\mathbb{D}_k$-module on which F and V are nilpotent, then $\mathcal{H}(M)$ is a k-vector space on which $F = V = 0$. The presentation of $M(w)$ by generators and relations makes it clear that if $w = v^{n_\ell} f^{m_\ell} \cdots v^{n_1} f^{m_1}$, then $\mathcal{H}(M(w))$ has dimension ℓ. More precisely, the images of the generators $E_0, \dots, E_{\ell-1}$ in $\mathcal{H}(M(w))$ are a basis.

Definition 5.3. If G is a finite group scheme over k killed by p, the *a-number of G*, denoted $a(G)$, is the largest integer a such that there is an injection $\alpha_p^a \hookrightarrow G$ of group schemes. If G is connected and unipotent, $p^{a(G)}$ equals the order of the foot of G. Similarly, if M is a $\mathbb{D}_k$-module of finite length, the *a-number of* M, denoted $a(M)$, is the largest integer a such that there is a surjection $M \twoheadrightarrow M(\alpha_p) = \mathbb{D}_k/(F, V)$ of $\mathbb{D}_k$-modules.

It is clear that the a-number is additive in direct sums and that $a(M(f)) = a(M(v)) = 0$.

Lemma 5.4. *The a-numbers of BT_1 modules have the following properties:*

(1) *If ℓ, $m_1, \ldots, m_\ell$, and $n_1, \ldots, n_\ell$ are positive integers, then $a(M(v^{n_\ell} f^{m_\ell} \cdots v^{n_1} f^{m_1})) = \ell$.*
(2) *Also $a(M(w))$ is the number of rotations of w which start with v and end with f.*

Proof. For part (1), $a(M) = \dim_k(\mathcal{H}(M))$ and, by the discussion above, if $w = v^{n_\ell} f^{m_\ell} \cdots v^{n_1} f^{m_1}$, then $a(M(w)) = \ell$. Part (2) is immediate from part (1). □

5.3. Homs from $G_{1,1}$. Write $M_{1,1} := \mathbb{D}_k/(F - V) \cong M(fv)$. Let $G_{1,1}$ be the BT_1 group scheme over k such that $M(G_{1,1}) \simeq M_{1,1}$. The group scheme $G_{1,1}$ appears "in nature" as the kernel of multiplication by p on a supersingular elliptic curve over k (e.g., see [Ulm91, Prop. 4.1]).

Definitions 5.5. Let G be a BT_1 group scheme over k and let M be a BT_1 module.

(1) Define the $s_{1,1}$-*multiplicity of* G as the largest integer $\mathfrak{s}$ such that there is an isomorphism of group schemes
$$G \cong G_{1,1}^{\mathfrak{s}} \oplus G'.$$
Define the $s_{1,1}$-*multiplicity of* M as the largest integer $\mathfrak{s}$ such that there is an isomorphism of $\mathbb{D}_k$-modules $M \cong M_{1,1}^{\mathfrak{s}} \oplus M'$.
(2) Define the $u_{1,1}$-*number of* G as the largest integer $\mathfrak{u}$ such that there exists an injection
$$G_{1,1}^{\mathfrak{u}} \hookrightarrow G$$
of group schemes. Define the $u_{1,1}$-*number of* M as the largest integer $\mathfrak{u}$ such that there is a surjection $M \twoheadrightarrow M_{1,1}^{\mathfrak{u}}$ of $\mathbb{D}_k$-modules.

The notation $s_{1,1}$ (resp. $u_{1,1}$) is motivated by the word superspecial (resp. unpolarized), see Section 5.5. Note the equalities $s_{1,1}(M(G)) = s_{1,1}(G)$ and $u_{1,1}(M(G)) = u_{1,1}(G)$. It is clear that $u_{1,1}(G) \geq s_{1,1}(G)$. The $s_{1,1}$-multiplicity and $u_{1,1}$-number are additive in direct sums.

By the Kraft classification, if $M(G)$ is described by a multiset of primitive cyclic words, then $s_{1,1}(G)$ equals the multiplicity of the cyclic word fv in the multiset.

We want to compute the $u_{1,1}$-number of the standard BT_1 modules $M(w)$. Trivially,
$$u_{1,1}(M(f)) = u_{1,1}(M(v)) = 0.$$

A straightforward exercise shows that $u_{1,1}(M(fv)) = 1$, and more precisely that

$$\mathrm{Hom}_{\mathbb{D}_k}(M(fv), M(fv)) \cong \mathbb{F}_{p^2} \times k,$$

with $(c, d) \in \mathbb{F}_{p^2} \times k$ identified with the homomorphism that sends the class of $1 \in \mathbb{D}_k/(F - V)$ to the class of $c + dF$. The surjective homomorphisms are those where $c \neq 0$.

We may thus assume that w has length $\lambda > 2$. We will evaluate the $u_{1,1}$-number of $M(w)$ by computing $\mathrm{Hom}_{\mathbb{D}_k}(M(w), M_{1,1})$ explicitly. To that end, write $w = v^{n_\ell} f^{m_\ell} \cdots v^{n_1} f^{m_1}$. Since $\lambda > 2$ and and w is non-periodic, we may replace w with a rotated word so that $m_1 > 1$ or $n_\ell > 1$ (or both). Roughly speaking, the following proposition says that the $u_{1,1}$-number of $M(w)$ is the number of appearances in w of subwords of the form $v^{>1}(fv)^e f^{>1}$ where $e \geq 0$. For example, if $w = v^2 f^2 v^3 f v f^4$, then the $u_{1,1}$-number is 2.

Proposition 5.6. *Suppose $w = v^{n_\ell} f^{m_\ell} \cdots v^{n_1} f^{m_1}$ where $m_1 > 1$ or $n_\ell > 1$. Define u by:*

$$\begin{aligned} u := &\# \{1 \leq i \leq \ell \mid m_i > 1 \text{ and } n_i > 1\} \\ &+ \# \{1 \leq i < j \leq \ell \mid n_j > 1,\ m_j = n_{j-1} = \cdots = n_i = 1,\ \text{and } m_i > 1\}. \end{aligned}$$

Then

1. *the $s_{1,1}$ number of $M(w)$ is ℓ if $m_i = n_i = 1$ for all i, and 0 otherwise,*
2. $\mathrm{Hom}_{\mathbb{D}_k}(M(w), M_{1,1})$ *is in bijection with $k^{u+\ell}$, and*
3. *the $u_{1,1}$-number of $M(w)$ is u.*

Proof. Part (1) follows from the fact that for a primitive word w, the $s_{1,1}$ number of $M(w)$ is 1 if $\overline{w} = \overline{fv}$ and is zero otherwise.

For part (2), we use Lemma 3.1 to present $M(w)$ with generators $E_0, \ldots, E_{\ell-1}$ (with indices taken modulo ℓ) and relations $F^{m_i} E_{i-1} = V^{n_i} E_i$. Let z_0, z_1 be a k-basis of $M_{1,1}$ with $Fz_0 = Vz_0 = z_1$ and $Fz_1 = Vz_1 = 0$. Then a homomorphism $\psi : M(w) \to M_{1,1}$ is determined by its values on the generators E_i. Write

$$\psi(E_i) = a_{i,0} z_0 + a_{i,1} z_1.$$

Then ψ is a $\mathbb{D}_k$-module homomorphism if and only if $F^{m_i}\psi(E_{i-1}) = V^{n_i}\psi(E_i)$ for $i = 1, \ldots, \ell$. By (2.1),

$$F^{m_i}\psi(E_{i-1}) = \begin{cases} a_{i-1,0}^p z_1 & \text{if } m_i = 1 \\ 0 & \text{if } m_i > 1 \end{cases}$$

and

$$V^{n_i}\psi(E_i) = \begin{cases} a_{i,0}^{1/p} z_1 & \text{if } n_i = 1 \\ 0 & \text{if } n_i > 1. \end{cases}$$

This system of equations places no constraints on $a_{i,1}$ for $i = 1, \ldots, \ell$, because $Vz_1 = Fz_1 = 0$. The constraints on $a_{i,0}$ for $i = 1, \ldots, \ell$ are: if $m_i = n_i = 1$, then $a_{i-1,0}^p = a_{i,0}^{1/p}$; if $m_i = 1$ and $n_i > 1$, then $a_{i-1,0} = 0$; if $m_i > 1$ and

$n_i = 1$, then $a_{i,0} = 0$; if $m_i > 1$ and $n_i > 1$, then no constraint. Using that $m_1 > 1$ or $n_\ell > 1$, we find a triangular system of equations for $a_{i,0}$, and it is a straightforward exercise to show that the solutions are in bijection with k^u. Combining with the k^ℓ unconstrained values of $\{a_{i,1} \mid 1 \leq i \leq \ell\}$ yields part (2).

For part (3), the homomorphism $\psi : M(w) \to M_{1,1}$ is surjective if and only if at least one of the $a_{i,0}$ is not zero, which is equivalent to ψ inducing a surjection $\mathcal{H}(M(w)) \to \mathcal{H}(M_{1,1}) = k$. Part (1) implies that there are u independent such ψ (and no more). This shows that u is the largest integer such that there is a surjection $M(w) \to M_{1,1}^u$, completing the proof of part (3). □

5.4. Motivation. The next proposition motivates the $s_{1,1}$-multiplicity and the $u_{1,1}$-number.

Proposition 5.7. *Let A/k be an abelian variety and let E/k be a supersingular elliptic curve.*

(1) *If there is an abelian variety B and an isogeny $E^s \times B \to A$ of degree prime to p, then s is less than or equal to the $s_{1,1}$-multiplicity of $A[p]$.*
(2) *If there is a morphism of abelian varieties $E^u \to A$ with finite kernel of order prime to p, then u is less than or equal to the $u_{1,1}$-number of $A[p]$.*

Proof. An isogeny as in (1) shows that $E[p] \cong G_{1,1}$ is a direct factor of $A[p]$ with multiplicity s, so $s \leq s_{1,1}(A[p])$. A morphism as in (2) shows that $E[p] \cong G_{1,1}$ appears in $A[p]$ with multiplicity at least u, so $u \leq u_{1,1}(A[p])$. □

5.5. Connection to the superspecial rank. Suppose G is a polarized BT_1 group scheme. In [AP15, Def. 3.3], Achter and Pries define the *superspecial rank* of G as the largest integer s such that there is an injection $G_{1,1}^s \hookrightarrow G$ and such that the polarization on G restricts to a non-degenerate pairing on $G_{1,1}^s$. In this situation, the pairing allows them to define a complement (see [AP15, Lemma 3.4]), so that $G \cong G_{1,1}^s \oplus G'$ (a direct sum of polarized BT_1 group schemes). A self-dual BT_1 group scheme G equipped with a decomposition $G \cong G_{1,1} \oplus G'$ (just of BT_1 group schemes) automatically admits a polarization compatible with the direct sum decomposition. Therefore, the superspecial rank of G equals its $s_{1,1}$-multiplicity.

They also define an *unpolarized superspecial rank*, which is the same as our $u_{1,1}$-number, and prove a result [AP15, Lemma 3.8] which is closely related to and implied by Proposition 5.6.

Next, we consider a correction to [AP15, Thm. 3.14]. Let K be the function field of an irreducible, smooth, proper curve X over k, let J_X be the Jacobian of X, and let E be a supersingular elliptic curve over k which we regard as a curve over K by base change. Let $\mathrm{Sel}(K, p)$ denote the Selmer group for the multiplication-by-p isogeny of E/K. See [Ulm91] for details.

Proposition 5.8. *With notation as above, let a, $u_{1,1}$, and $s_{1,1}$ be the a-number, $u_{1,1}$-number, and $s_{1,1}$-multiplicity of $J_X[p]$ respectively. Then the group* $\mathrm{Sel}(K,p)$ *is isomorphic to the product of a finite group and a k-vector space of dimension $a+u_{1,1}-s_{1,1}$.*

Proof. Applying [Ulm19, Props. 6.2 and 6.4] with $\mathcal{C}=X$, $\mathcal{D}=E$, $\Delta=1$, and $n=1$ shows that $\mathrm{Sel}(K,p)$ and $\mathrm{Hom}_{\mathbb{D}}(H^1_{dR}(X),M_{1,1})$ differ by a finite group. By [Oda69, Cor. 5.11], $H^1_{dR}(X)\cong M(J_X[p])$. Write $M(J_X[p])$ as a sum of indecomposable BT_1 modules $M(w)$ for suitable cyclic words w. In Section 4.3, we computed $H_w=\mathrm{Hom}_{\mathbb{D}}(M(w),M_{1,1})$ for a primitive cyclic word w. Recall that $H_w=0$ if $w=f$ or $w=v$ and $H_w\cong\mathbb{F}_{p^2}\times k$ if $w=fv$. Also $H_w\cong k^{u+\ell}$, if $w\notin\{1,f,v,fv\}$ where $u=u_{1,1}(M(w))$ and ℓ is the a-number of $M(w)$. The result follows from the additivity of a-numbers, $u_{1,1}$-numbers, and $s_{1,1}$-multiplicities. □

Next, we compute the numerical invariants of a module $M=\oplus M(\overline{w}_i)^{m_i}$ in terms of multiplicities of words. In Section 3.5, we defined multiplicities μ by considering all lifts of $\overline{w}_i$ to words and taking powers of those words so they all have the same length $\ell=\mathrm{lcm}(\text{lengths of }\overline{w}_i)$. Let $\mu(f\text{—}v)$ be the sum of the multiplicities of all these words of length ℓ starting with f and ending with v; and let $\mu(\text{—}vf)$ be the sum of the multiplicities of all words of length ℓ ending with vf.

Proposition 5.9. *The BT_1 module $M=\oplus M(\overline{w}_i)^{m_i}$ has*

1. *p-rank equal to $\mu(f^\ell)$,*
2. *a-number equal to $\mu(f\text{—}v)=\mu(\text{—}vf)=\mu(\text{—}fv)$,*
3. *$s_{1,1}$-multiplicity equal to $\mu((fv)^{\ell/2})$ if ℓ is even and to 0 if ℓ is odd,*
4. *and $u_{1,1}$-number equal to the sum of the $s_{1,1}$ multiplicity and*

$$\mu(\text{—}v^2f^2)+\mu(\text{—}v^2fvf^2)+\cdots+\mu(\text{—}v^2(fv)^{\lfloor(\ell-4)/2\rfloor}f^2).$$

Proof. Parts (1) and (2) follow from Lemma 5.2 and Lemma 5.4 respectively. Parts (3) and (4) follow from Proposition 5.6. □

5.6. Examples. For small genus, we give tables of elementary sequences ("E–O"), matched with the self-dual multisets of primitive cyclic words ("K"), together with their p-ranks, a-numbers, $s_{1,1}$-multiplicities, and $u_{1,1}$-numbers.

From Section 4.2.1, for the BT_1 module of the elementary sequence $\Psi=[\psi_1,\ldots,\psi_g]$, the p-rank is the largest i such that $\psi_i=i$ and the a-number is $g-\psi_g$. We do not know how to compute the $s_{1,1}$-multiplicity or $u_{1,1}$-number directly from Ψ.

For the BT_1 module of a multiset of cyclic words, the p-rank is the multiplicity of the word f by Lemma 5.2 and the a-number can be computed using Lemma 5.4. The $s_{1,1}$-multiplicity is the multiplicity of the cyclic word fv and the $u_{1,1}$-number can be computed using Proposition 5.6.

$g=1$					
E–O	K	p-rank	a-number	$s_{1,1}$-mult.	$u_{1,1}$-number
$[0]$	$\{fv\}$	0	1	1	1
$[1]$	$\{f,v\}$	1	0	0	0

$g=2$					
E–O	K	p-rank	a-number	$s_{1,1}$-mult.	$u_{1,1}$-number
$[0,0]$	$\{(fv)^2\}$	0	2	2	2
$[0,1]$	$\{ffvv\}$	0	1	0	1
$[1,1]$	$\{f,v,fv\}$	1	1	1	1
$[1,2]$	$\{(f)^2,(v)^2\}$	2	0	0	0

If G is a polarized BT_1 group scheme of order p^{2g} with positive p-rank, then $G \cong G' \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mu_p$ where G' is a polarized BT_1 group scheme of order p^{2g-2}. Thus the rows of the table for g for G with positive p-rank can be deduced from the table for $g-1$. In passing from genus $g-1$ to genus g: the elementary sequence changes from $[\psi_1,\dots,\psi_{g-1}]$ to $[1,\psi_1+1,\dots,\psi_{g-1}+1]$; the multiplicity of the words f and v increases by 1; the p-rank increases by 1; and the a-number, $s_{1,1}$-multiplicity, and $u_{1,1}$-number stay the same. In light of this, when $g=3$ and $g=4$, we only include the BT_1 group schemes with p-rank 0 in the table.

$g=3$					
E–O	K	p-rank	a-number	$s_{1,1}$-mult.	$u_{1,1}$-number
$[0,0,0]$	$\{(fv)^3\}$	0	3	3	3
$[0,0,1]$	$\{fv,ffvv\}$	0	2	1	2
$[0,1,1]$	$\{fvv,vff\}$	0	2	0	0
$[0,1,2]$	$\{fffvvv\}$	0	1	0	1

The E–O structure $[0,1,1]$ is the first which is decomposable as a BT_1 group scheme but indecomposable as a polarized BT_1 group scheme.

$g=4$					
E–O	K	p-rank	a-number	$s_{1,1}$-mult.	$u_{1,1}$-number
$[0,0,0,0]$	$\{(fv)^4\}$	0	4	4	4
$[0,0,0,1]$	$\{(fv)^2,ffvv\}$	0	3	2	3
$[0,0,1,1]$	$\{ffvfvvfv\}$	0	3	0	1
$[0,0,1,2]$	$\{(ffvv)^2\}$	0	2	0	2
$[0,1,1,1]$	$\{fv,ffv,vvf\}$	0	3	1	1
$[0,1,1,2]$	$\{fv,fffvvv\}$	0	2	1	2
$[0,1,2,2]$	$\{fffv,fvvv\}$	0	2	0	0
$[0,1,2,3]$	$\{ffffvvvv\}$	0	1	0	1

6. Fermat Jacobians

In this section, we recall two results on the BT_1 modules of Fermat curves from [PU].

For each positive integer d not divisible by p, let F_d be the Fermat curve of degree d, i.e., the smooth, projective curve over k with affine model

$$F_d : \qquad X^d + Y^d = 1,$$

and let J_{F_d} be its Jacobian. Let $\mathcal{C}_d$ be the smooth, projective curve over k with affine model

$$\mathcal{C}_d : \qquad y^d = x(1-x). \tag{6.1}$$

The substitution X^d for x and XY for y in the equation for $\mathcal{C}_d$ shows that $\mathcal{C}_d$ is a quotient of F_d. The map $F_d \to \mathcal{C}_d$ is the quotient of F_d by the subgroup

$$\{(\zeta, \zeta^{-1}) \mid \zeta \in \mu_d\} \subset (\mu_d)^2 \subset \operatorname{Aut}(F_d)$$

of index d. The Riemann-Hurwitz formula shows that the genus of $\mathcal{C}_d$ is

$$g(\mathcal{C}_d) = \lfloor (d-1)/2 \rfloor = \begin{cases} (d-1)/2 & \text{if } d \text{ is odd,} \\ (d-2)/2 & \text{if } d \text{ is even.} \end{cases}$$

Theorem 6.1 (=[PU, Thm. 5.5]). *The Dieudonné module $M(J_d[p])$ is the BT_1 module with data*

$$S = \mathbb{Z}/d\mathbb{Z} \setminus \{0, d/2\} \text{ if } d \text{ is even, and } S = \mathbb{Z}/d\mathbb{Z} \setminus \{0\} \text{ if } d \text{ is odd,}$$

$$S_f = \{a \in S \mid d/2 < a < d\}, \quad S_v = \{a \in S \mid 0 < a < d/2\},$$

and the permutation $\pi : S \to S$ given by $\pi(i) = pa$.

Theorem 6.2 (=[PU, Thm. 5.9]). *The Dieudonné module $M(J_{F_d}[p])$ is the BT_1 module with data*

$$T = \left\{(a,b) \in (\mathbb{Z}/d\mathbb{Z})^2 \mid a \neq 0, b \neq 0, a+b \neq 0\right\},$$

$$T_f = \{(a,b) \in S \mid a+b > d\}, \quad T_v = \{(a,b) \in S \mid a+b < d\},$$

and the permutation $\sigma(a,b) = (pa, pb)$.

Remark 6.3. Let μ_d be the group of d-th roots of unity in k, and note that μ_d acts on $\mathcal{C}_d$ by multiplication on the y coordinate. Although this action does not appear explicitly in Theorem 6.1, it plays a key role in the proof. Indeed, the k-valued characters of μ_d can be identified with $\mathbb{Z}/d\mathbb{Z}$, and the set S is precisely the set of characters of μ_d which appear in $H^1_{dR}(\mathcal{C}_d)$. Each character that appears does so with multiplicity one. The subset S_v consists of those characters appearing in the subspace $H^0(\mathcal{C}_d, \Omega^1) \subset H^1_{dR}(\mathcal{C}_d)$. Moreover, the indecomposable submodules of $M(J_d[p])$ as a BT_1 module with μ_d action correspond to the orbits of p on S. As noted in [PU, Rem. 5.6], such a submodule may become decomposable if we ignore the μ_d action.

Remark 6.4. The action of μ_d also allows one to decompose the Jacobian J_d (i.e., the motive of $\mathcal{C}_d$) into parts indexed by divisors of d. If d' divides d, there is a projection $\mathcal{C}_d \to \mathcal{C}_{d'}$ and an induced inclusion $J_{d'} \to J_d$. Defining J_d^{new} as the quotient of J_d by the sum of the images of $J_{d'} \to J_d$ where d' runs through proper divisors of d, we obtain an isogeny

$$J_d \sim \bigoplus_{d'|d} J_{d'}^{new}$$

of degree prime to p. In particular, the p-divisible group of J_d is isomorphic to the direct sum of the p-divisible groups of the $J_{d'}^{new}$. For $d = 1$ and $d = 2$, J_d^{new} is trivial; if $d > 2$, then J_d^{new} is an abelian variety with complex multiplication by the cyclotomic field $\mathbb{Q}(\mu_d)$. A slight generalization of the proof of Theorem 6.1 allows one to compute the CM type of J_d^{new}. Using this, one finds that the p-divisible group of J_d^{new} is a "standard ordinary" in the sense of [Moo04, 1.2.3]. See also [PU, Rem. 5.10].

Remark 6.5. The quotient $\mathcal{C}_d \to F_d$ induces an inclusion $S \hookrightarrow T$ sending a to (a, a), and the partition and permutation of T are compatible with those of S. There are other quotients $\mathcal{C}$ of F_d by subgroups of μ_d^2. (For example, the curves $v^e = u^r(1-u)^s$ where $e \mid d$, $\gcd(r, s, e) = 1$, and $r + s < e$.) Each gives rise to a set $S_{\mathcal{C}}$ with partition and permutation and the projection $F_d \to \mathcal{C}$ induces an inclusion $S_{\mathcal{C}} \hookrightarrow T$ compatible with the partitions and permutations. The interesting features of $J_{F_d}[p]$ are already present in $J_{\mathcal{C}_d}[p]$, so we restrict to studying this case for simplicity.

7. Ekedahl–Oort structures of Fermat quotients: general case

In this section, we determine the Ekedahl–Oort type of the Jacobian J_d of the Fermat quotient curve $\mathcal{C}_d$ with affine model $y^d = x(1-x)$ for d relatively prime to p.

7.1. Words, patterns, and multiplicities. By Theorem 6.1, the BT_1 module of $J_d[p]$ is the one obtained from diagram (3.1) using the data $S \subset \mathbb{Z}/d\mathbb{Z}$ with its usual partition and permutation. This data gives rise to a multiset of cyclic words. To compute the E–O structure, as in Section 3.5, we consider all representative words of the cyclic words, take powers so they all have the same length, and compute their multiplicities to find the dimensions of the blocks $B_i = M_{i+1}/M_i$ in the canonical filtration.

We want to reformulate this to go directly from the set S to the multiplicities μ. To do so, we introduce the *pattern* of an element of S. This is a variant of the word which takes into account the powers mentioned in the previous paragraph.

Let $\ell = |\langle p\rangle|$ be the multiplicative order of p modulo d. Let $\mathcal{W}_\ell$ be the set of words of length ℓ on $\{f, v\}$. Define a map $\mathrm{Pat} : S \to \mathcal{W}_\ell$ as follows: for

$a \in S$, define $\mathrm{Pat}(a) = u_{\ell-1} \cdots u_0$ where

$$u_j = f \text{ if } p^j a \in S_f, \text{ and } u_j = v \text{ if } p^j a \in S_v.$$

If the word w_a for a has length ℓ (which happens when $\gcd(a, d) = 1$), then $\mathrm{Pat}(a) = w_a$ whereas for a with a shorter word, $\mathrm{Pat}(a)$ is a power of w_a.

For example, take $d = 9$ and $p = 2$, so that $\ell = 6$. The orbits of $\langle p \rangle$ are $1 \to 2 \to 4 \to 8 \to 7 \to 5 \to 1$ and $3 \to 6 \to 3$. For $a = 3$, the word is fv and $\mathrm{Pat}(3) = fvfvfv$. For $a = 6$, the word is vf and $\mathrm{Pat}(6) = vfvfvf$. For $a \neq 3, 6$, then $\mathrm{Pat}(a) = w_a$; for example $\mathrm{Pat}(1) = fffvvv$.

For $w \in \mathcal{W}_\ell$, define the *multiplicity* of w to be the cardinality of its inverse image under Pat:

$$\mu(w) := \left|\mathrm{Pat}^{-1}(w)\right|.$$

This is the same multiplicity as defined in Section 3.5 for the module determined by S.

7.2. Ekedahl–Oort structure of $J_d[p]$. Recall from Section 4.2.1 that the E–O structure associated to a self-dual BT_1 module is the sequence of integers $[\psi_1, \ldots, \psi_g]$ which starts from $\psi_0 = 0$ and has sections of length equal to the block sizes $\dim(B_i)$ which are increasing (resp. constant) if the word attached to the block ends with f (resp. v).

To simplify this description, we introduce some notation: $\nearrow^m$ (resp. $\to^m$) stands for an increasing (resp. constant) sequence of integers of length m. Thus,

$$[\nearrow^3 \to^2] = [1, 2, 3, 3, 3] \quad \text{and} \quad [\to^2 \nearrow^3] = [0, 0, 1, 2, 3].$$

Now enumerate the elements of $\mathcal{W}_\ell$ that start with f in lexicographic order:

$$w_0 = f^\ell,\ w_1 = f^{\ell-1}v,\ w_2 = f^{\ell-2}vf,\ w_3 = f^{\ell-2}vv,\ \ldots,\ w_{2^{\ell-1}-1} = fv^{\ell-1}. \tag{7.1}$$

Let $\mu_j = \mu(w_j)$.

Using Sections 3.5 and 4.2.1, we get the following description of the E–O structure of $J_d[p]$:

Theorem 7.1. *Let ℓ be the multiplicative order of p modulo d, and let $\mu_0, \ldots, \mu_{2^{\ell-1}-1}$ be the multiplicities of the words above. Let J_d be the Jacobian of the Fermat quotient curve C_d with affine model $y^d = x(1-x)$. The Ekedahl–Oort structure of $J_d[p]$ is given by*

$$[\nearrow^{\mu_0} \to^{\mu_1} \nearrow^{\mu_2} \cdots \to^{\mu_{2^{\ell-1}-1}}].$$

Proof. Indeed, for the BT_1 module $M = M(J_d[p])$ and for $0 \leq j < 2^{\ell-1}$, the subspace M_{j+1} in the canonical filtration is the span of the basis vectors e_a indexed by $a \in S$ such that $\mathrm{Pat}(a) \leq w_j$. In particular, $\dim(M_{j+1}) = \sum_{i=0}^{j} \mu_i$. By Definition 3.2, $B_j = M_{j+1}/M_j$, so $\dim(B_j) = \mu_j$. If j is even, then w_j ends with f so B_j is mapped isomorphically onto its image by F. If j is odd, then w_j ends with v so B_j is killed by F. Thus the μ_j are the values of $\rho(j+1) - \rho(j)$ in the canonical type of $J_d[p]$, and they give the lengths of the runs where the elementary sequence is increasing (j even) or constant (j odd). □

8. Ekedahl–Oort structures of Fermat quotients: the case $p = 2$

In this section, suppose $p = 2$. In this case, the curve $\mathcal{C}_d$ is an Artin-Schreier cover of the projective line with equation $x^2 - x = y^d$, and the formulas when $p = 2$ are different from the case when p is odd. We do not include proofs in this section because most of the results already appear in the literature.

The genus of $\mathcal{C}_d$ is $g_d = (d-1)/2$.

Corollary 8.1. *Let $p = 2$ and $d > 1$ be odd. Let J_d be the Jacobian of $\mathcal{C}_d : y^d = x(1-x)$. Then:*

(1) [EP13, special case of Thm. 1.3] *the Ekedahl–Oort type of $J_d[2]$ has the form*
$$[0, 1, 1, 2, 2, \ldots, \lfloor g_d/2 \rfloor].$$
(2) [Sub75, Theorem 4.2] *(Deuring-Shafarevich formula) the 2-rank of $J_d[2]$ is 0;*
(3) [EP13, Prop. 3.4] *the a-number of $J_d[2]$ is $\frac{d-1}{4}$ if $d \equiv 1 \pmod 4$ and $\frac{d+1}{4}$ if $d \equiv 3 \pmod 4$;*
(4) [AP15, Application 5.3] *the $s_{1,1}$-multiplicity of $J_d[2]$ is 1 if $d \equiv 0$ mod 3 and is 0 otherwise.*

9. The a-number of the Fermat quotient curve

Suppose p is odd. Let J_d be the Jacobian of the curve $\mathcal{C}_d$ with affine model $y^d = x(1-x)$. We find a closed-form formula for the a-number of J_d and some information about its p-rank.

If $d = 1, 2$, then $\mathcal{C}_d$ is rational; we exclude this trivial case in the next results.

Proposition 9.1. *Suppose p is odd, $d > 2$, and p does not divide d. Then:*

(1) *The a-number of $J_d[p]$ is*
$$\sum_{j=1}^{(p-1)/2} \left(\left\lfloor \frac{2jd}{2p} \right\rfloor - \left\lfloor \frac{(2j-1)d}{2p} \right\rfloor \right)$$
$$= \frac{(p-1)}{p}\frac{d}{4} - \sum_{j=1}^{(p-1)/2} \left(\left\langle \frac{2jd}{2p} \right\rangle - \left\langle \frac{(2j-1)d}{2p} \right\rangle \right).$$
Here $\langle \cdot \rangle$ denotes the fractional part.

(2) *If $d \equiv \pm 1 \pmod{2p}$, then the a-number of J_d is*
$$(p-1)(d \mp 1)/4p.$$

(3) *If* $d \equiv p \pm 1 \pmod{2p}$, *then the a-number of* J_d *is*

$$(p-1)(d \pm (p-1))/4p.$$

Remark 9.2. An analogue of parts (2) and (3) for the Fermat curve F_d was proven by Montanucci and Speziali [MonS18] using the Cartier operator.

Proof. By Proposition 5.9, the a-number of $J_d[p]$ is $\mu(—fv)$ which equals $\mu(—vf)$ since $J_p[d]$ is self-dual. This is the number of elements $a \in S$ such that the pattern of a ends with fv. These are precisely the elements with $a \in S_v$ and $pa \in S_f$, and we may count them using archimedean considerations. More precisely, $a \in S_v$ means $0 < a < d/2$ and $pa \in S_f$ means that (the least positive residue of) pa satisfies $d/2 < pa < d$.

We prove part (1) and leave the other parts as exercises. The elements of S which contribute to the a-number are represented by integers satisfying one of the inequalities

$$\frac{d}{2p} < a < \frac{2d}{2p}, \quad \frac{3d}{2p} < a < \frac{4d}{2p}, \quad \dots, \quad \frac{(p-2)d}{2p} < a < \frac{(p-1)d}{2p},$$

and the number of such integers is the left hand side of the displayed equation in part (1). The equality in the displayed equation in part (1) is immediate from the definitions of $\lfloor . \rfloor$ and $\langle . \rangle$. □

Remark 9.3. If p is large and d is large with respect to p, by Proposition 9.1, the a-number of J_d is close to $\frac{(p-1)}{p}\frac{d}{4}$ which is close to $g/2$. The second expression in part (1) shows that the difference is less than $(p-1)/2$ in absolute value. Numerical experiments suggest that the difference is bounded by $\frac{(p-1)^2}{4p}$ and part (3) shows that the difference equals this when $d \equiv p \pm 1 \pmod{2p}$.

An abelian variety A is *superspecial* if its a-number is equal to its dimension. This is equivalent to A being isomorphic to a product of supersingular elliptic curves. The next result shows that J_d is superspecial if and only if $\mathcal{C}_d$ is a quotient of $\mathcal{C}_{p+1}$ by a subgroup of μ_{p+1}.

Proposition 9.4. *Suppose* $d > 2$ *and* $p \nmid d$. *Then* J_d *is superspecial if and only if* d *divides* $p+1$.

An analogue of Proposition 9.4 for F_d was proven by Kodama and Washio [KoW88, Cor. 1, p. 192]. The "if" direction of our proposition follows from their result.

Proof. By Proposition 5.9(2), J_d is superspecial if and only if $\mu((fv)^{g/2}) = g$. This is the case if and only if p exchanges S_f and S_v, i.e., $pS_f = S_v$ and $pS_v = S_f$. Note also that if this statement holds for (p, d) then it holds for (p, d') for any divisor $d' > 2$ of d.

We claim that if $H \subset (\mathbb{Z}/d\mathbb{Z})^\times$ is a subgroup such that $hS_v = S_v$ (equivalently $hS_f = S_f$) for all $h \in H$, then $H = \{1\}$. Suppose that H is such a subgroup, $1 < a < d$, and the class of a lies in H. If $a > d/2$, then a sends

$1 \in S_v$ to $a \notin S_v$, a contradiction. If $a < d/2$, then there is an integer b in the interval $(d/2a, d/a)$, so $b \in S_v$, and $d/2 < ab < d$, so the class of ab lies in S_f, again a contradiction. Thus $H = \{1\}$.

Suppose that p exchanges S_f and S_v. By applying the claim to $H = \langle p^2 \rangle$, we see that p has order 2 modulo d, and the same holds for p modulo d' for any divisor d' of d. Since 1 does not exchange S_f and S_v, the order of p is exactly 2 modulo any $d' > 2$ dividing d. If d' is an odd prime power, this implies $p \equiv -1 \pmod{d'}$.

More generally, let $d' = 2^e$ be the largest power of 2 dividing d. If $d' = 1$ or 2, then $p \equiv -1 \pmod{d'}$. If $d' = 4$, there is a unique class of order exactly 2 modulo d', namely -1, and again $p \equiv -1 \pmod{d'}$. Finally, if $e > 2$, then there are three elements of order exactly 2 modulo d', but only one of them reduces to an element of order 2 modulo 2^{e-1}, namely -1. Again, we find $p \equiv -1 \pmod{d'}$. In all three cases, $p \equiv -1 \pmod{d'}$ and so $p \equiv -1 \pmod{d}$, as required. □

9.1. Observations about the p-rank. The behavior of the p-rank, $s_{1,1}$-multiplicity, and $u_{1,1}$-number of J_d for arbitrary p and d seems rather erratic. In later sections, we give closed form formulas for these invariants under restrictions on d. Here we include some observations about when the p-rank is as large or small as possible.

An abelian variety is *ordinary* if its p-rank is equal to its dimension. The next result shows that J_d is ordinary if and only if $\mathcal{C}_d$ is a quotient of $\mathcal{C}_{p-1}$ by a subgroup of μ_{p-1}.

Proposition 9.5. *Suppose $d > 2$ and $p \nmid d$. Then J_d is ordinary if and only if d divides $p - 1$.*

An analogue of Proposition 9.5 for the Fermat curve F_d was proven by Yui [Yui80, Thm. 4.2] using exponential sums; (see also [Gon97, Prop 5.1] for a proof using the Cartier operator when d is prime). The "if" direction of our proposition can be deduced from Yui's result.

Proof. By Proposition 5.9(1), J_d is ordinary if and only if $\mu(f^\ell) = g$. If d divides $p - 1$, then $\ell = 1$, the orbits of $\langle p \rangle$ on $S \subset \mathbb{Z}/d\mathbb{Z}$ are singletons, and $\mu(f) = |S_f| = g$, so J_d is ordinary.

The converse follows from the claim in the proof of Proposition 9.4. □

At the opposite extreme, the p-rank of J_d is 0 when d divides $p + 1$, by Proposition 9.4. If J_d is supersingular, then the p-rank of J_d is zero (the converse is not necessarily true for $g \geq 3$); by [Gon97, Prop. 5.1], J_d is supersingular when d is prime and the order of p in $(\mathbb{Z}/d\mathbb{Z})^\times$ is even.

9.2. Breaks in words. We end this section with an elementary combinatorial result used later.

Fix d and let ℓ be the order of $\langle p \rangle \subset (\mathbb{Z}/d\mathbb{Z})^\times$. Given a pattern of length ℓ, say $w = u_{\ell-1} \cdots u_0$, we say that $0 \leq j < \ell - 1$ is a *break* of w if $u_{j+1} \neq u_j$, and we say $j = \ell - 1$ is a break of w if $u_0 \neq u_{\ell-1}$. If k is the number of breaks of w, then k is even and $0 \leq k \leq \ell$. Moreover, a pattern w is determined by its set of breaks and by its last letter u_0, and there are $2\binom{\ell}{k}$ words of length ℓ with k breaks. The sum of these numbers for $0 \leq k \leq \ell$ equals 2^ℓ.

We also consider "self-dual" words of length $\ell = 2\lambda$, i.e., words of the form $w^c \cdot w$ where w has length λ. Such a word is determined by its last half w, and we may encode w by specifying its last letter and its "breaks" as above, ignoring the last potential break: If $w = u_{\lambda-1} \cdots u_0$ we say that $0 \leq j < \lambda - 1$ is a *break* if $u_{j+1} \neq u_j$. (We ignore $j = \lambda - 1$ because whether or not $u_{\lambda-1}$ is a break of $w^c \cdot w$ is already determined by the other data.) There are $2\binom{\lambda-1}{k}$ words w with k breaks. The sum of these numbers for $0 \leq k \leq \lambda - 1$ is 2^λ.

Fix $\ell \geq 1$. As in (7.1), list all words of length ℓ which begin with f in lexicographic order:

$$w_0 = f^\ell, w_1 = f^{\ell-1}v, w_2 = f^{\ell-2}vf, \ldots, w_{2^{\ell-1}-1} = fv^{\ell-1}.$$

Let $k(i)$ be the number of breaks of w_i (not looking at possible wrap-around breaks).

Lemma 9.6. *The function $k(i)$ has the properties:* (i) $k(0) = 0$*; and* (ii) *if $2^j \leq i < 2^{j+1}$, then $k(i) = k(2^{j-1} - 1 - i) + 1$, and it is characterized by these properties.*

Proof. Clearly $k(0) = 0$. In the list of words, w_i is the binary representation of the integer i where f stands for 0, v stands for 1, and the leftmost letters are the most significant digits. Thus, if $2^j \leq i < 2^{j+1}$, then $w_i = f^{\ell-j-1}vt$ and $w_{2^{j-1}-1-i} = f^{\ell-j}(t^c)$ for some t, and it is visible that w_i has one more break than $w_{2^{j-1}-1-i}$ does. This proves the second property of k. The two properties clearly characterize k. □

The function $i \mapsto k(i)$ is independent of ℓ if $2^{\ell-1} > i$. Its first few values are:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$k(i)$	0	1	2	1	2	3	2	1	2	3	4	3	2	3	2	1

10. $J_d[p]$ in the "encompassing" case

Suppose p is odd. In this section, we fix $d = p^\ell - 1$, which we call the "encompassing" case. The reason is that if $p \nmid d'$, then d' divides $p^\ell - 1$ for some ℓ, with the quotient $(p^\ell - 1)/d'$ being prime-to-p, and so $J_{d'}[p]$ is a direct factor of $J_{p^\ell-1}[p]$. Let $S = S_f \cup S_v$ and π be defined as before.

10.1. p-adic digits. Elements $a \in S$ correspond to p-adic expansions

$$a = a_0 + a_1 p + \cdots + a_{\ell-1}p^{\ell-1}. \qquad (10.1)$$

where $a_i \in \{0, \ldots, p-1\}$ and we exclude the following cases: all $a_i = 0$ (when $a = 0$); all $a_i = p - 1$ (when $a = d$); and the case all $a_i = (p-1)/2$

(when $a = d/2$). Multiplication by p corresponds to permuting the digits cyclically.

10.2. Multiplicities. Given $a \in S$, let $\operatorname{Pat}(a) = u_{\ell-1} \cdots u_0$ be the pattern of a. Let (10.1) be the p-adic expansion of a. Then $a \in S_v$ (meaning $u_0 = v$) if and only if $a < d/2$. In other words, the condition is that the first p-adic digit to the left of $a_{\ell-1}$ (inclusive) which is not $(p-1)/2$ is in fact less than $(p-1)/2$.

Similarly $a \in S_f$ (meaning $u_0 = f$) if and only if $a > d/2$. This is true if and only if the first p-adic digit to the left of $a_{\ell-1}$ (inclusive) which is not $(p-1)/2$ is in fact greater than $(p-1)/2$. The other letters u_j of $\operatorname{Pat}(a)$ are determined similarly by looking at the p-adic digits of a to the left of $a_{\ell-1-j}$. (Finding the first digit $\neq (p-1)/2$ may require wrapping around.)

For example, if $\ell = 4$ and $p > 3$, then $\operatorname{Pat}(a) = ffvf$ when

$$a = (p-1)/2 + (p-2)p + 0p^2 + (p-2)p^3.$$

The following proposition records the "multiplicities" of each pattern.

Proposition 10.1. *Let p be odd and $d = p^\ell - 1$ and define $S = S_f \cup S_v$ as usual.*

(1) *For $w \in \mathcal{W}_\ell$, write $\mu(w)$ for the number of elements $a \in S$ with $\operatorname{Pat}(a) = w$. Then*

$$\mu(f^\ell) = \mu(v^\ell) = \left(\frac{p+1}{2}\right)^\ell - 2.$$

If w has $k > 0$ breaks, then

$$\mu(w) = \left(\frac{p-1}{2}\right)^k \left(\frac{p+1}{2}\right)^{\ell-k}.$$

(2) *More generally,*

$$\mu(\text{—}f^e) = \mu(\text{—}v^e) = \left(\frac{p+1}{2}\right) p^{\ell-e} - 2,$$

$$\begin{aligned}\mu(\text{—}v^{e_k} \cdots f^{e_1}) &= \mu(\text{—}f^{e_k} \cdots v^{e_1}) \\ &= \left(\frac{p+1}{2}\right)^{\sum e_j - k} \left(\frac{p-1}{2}\right)^{k-1} \left(\frac{p^{\ell+1-\sum e_j} - 1}{2}\right),\end{aligned}$$

and

$$\begin{aligned}\mu(\text{—}f^{e_{k+1}} v^{e_k} \cdots f^{e_1}) &= \mu(\text{—}v^{e_{k+1}} f^{e_k} \cdots v^{e_1}) \\ &= \left(\frac{p+1}{2}\right) p^{\sum e_j - k - 1} \left(\frac{p-1}{2}\right)^k \left(\frac{p^{\ell+1-\sum e_j} + 1}{2}\right).\end{aligned}$$

Proof. We prove part (1) and leave part (2) for the reader. The number of elements $a \in S$ whose pattern is f^ℓ or v^ℓ is $(\frac{p+1}{2})^\ell - 2$. Indeed, for f^ℓ (resp. v^ℓ), we may choose each a_j freely with $(p-1)/2 \le a_j \le p-1$ (resp. $0 \le a_j \le (p-1)/2$) except that we may not take them all to be $(p-1)/2$ nor all $p-1$ (resp. 0). This proves the first claim in (1).

Suppose w is a pattern with breaks. Then the inequalities at the beginning of this subsection show that an element a with pattern w should have digits a_j satisfying:

$$\begin{cases} a_j \le (p-1)/2 & \text{if } u_{\ell-1-j} = v \text{ and } j \text{ is not a break of } w, \\ a_j < (p-1)/2 & \text{if } u_{\ell-1-j} = v \text{ and } j \text{ is a break of } w, \\ a_j \ge (p-1)/2 & \text{if } u_{\ell-1-j} = f \text{ and } j \text{ is not a break of } w, \\ a_j > (p-1)/2 & \text{if } u_{\ell-1-j} = f \text{ and } j \text{ is a break of } w. \end{cases}$$

The count displayed in the second claim in (1) is then immediate. □

Theorem 10.2. *Let p be odd and $d = p^\ell - 1$. Let $\mathcal{C}_d$ be the curve $y^d = x(1-x)$ and let J_d be its Jacobian. Then the Ekedahl–Oort type of J_d has the form*

$$[\nearrow^{\mu_0} \rightarrow^{\mu_1} \cdots \rightarrow^{\mu_{2^{\ell-1}-1}}]$$

where $\mu_0 = (\frac{p+1}{2})^\ell - 2$ and for $1 \le i \le 2^{\ell-1} - 1$, letting $k(i)$ be the function in Lemma 9.6,

$$\mu_i = \begin{cases} \left(\frac{p-1}{2}\right)^{k(i)} \left(\frac{p+1}{2}\right)^{\ell-k(i)} & \text{if } i \text{ is even,} \\ \left(\frac{p-1}{2}\right)^{k(i)+1} \left(\frac{p+1}{2}\right)^{\ell-k(i)-1} & \text{if } i \text{ is odd.} \end{cases}$$

Proof. This follows immediately from Theorem 7.1, the calculation of multiplicities in Proposition 10.1, and the evaluation of the number of breaks in Lemma 9.6. (One should note that the k appearing in Proposition 10.1 for w_i is $k(i)$ if i is even, and it is $k(i)+1$ if i is odd.) □

10.3. Examples. Suppose p is odd.

(1) If $\ell = 1$, $\mathcal{C}_d$ has genus $(p-3)/2$ and is ordinary. The list of words as at (7.1) is just f. The elementary sequence is

$$[\nearrow^{(p-3)/2}] = [1, 2, \ldots, (p-3)/2].$$

(2) If $\ell = 2$, the list of words is ff, fv. The elementary sequence has an increasing section of length $(p+1)^2/4 - 2$ and a constant section of length $(p-1)^2/4$, i.e., it is:

$$[\nearrow^{(p+1)^2/4-2} \rightarrow^{(p-1)^2/4}]$$
$$= [1, 2, \ldots, (p+1)^2/4 - 2, \ldots, (p+1)^2/4 - 2].$$

(3) If $\ell = 3$, the list of words is f^3, f^2v, fvf, fvv. The elementary sequence is:

$$[\nearrow^m \rightarrow^n \nearrow^n \rightarrow^n],$$

where $m = (p+1)^3/8 - 2$ and $n = (p+1)(p-1)^2/8$.

(4) If $\ell = 4$, the word $f^3 v$ occurs; this is the smallest example whose BT_1 group scheme was not previously known to occur as a factor of the p-torsion of a Jacobian for all primes p. If $p \equiv 2, 3 \bmod 5$, then this group scheme occurs generically for the family of genus 4 curves that are degree 5 cyclic covers of $\mathbb{P}^1$ given by an equation of the form $y^5 = x(x-1)(x-\lambda)$, see [LMPT19, Notation 6.3, Theorem 7.3].

Proposition 10.3. *Let p be odd and let $d = p^\ell - 1 > 2$. Then:*

(1) *the p-rank of $J_d[p]$ is $(\frac{p+1}{2})^\ell - 2$;*
(2) *the a-number of $J_d[p]$ is $\frac{p-1}{2}\frac{p^{\ell-1}-1}{2}$;*
(3) *the $s_{1,1}$-multiplicity of $J_d[p]$ is 0 if ℓ is odd and is $(\frac{p^2-1}{4})^{\ell/2}$ if ℓ is even;*
(4) *and the $u_{1,1}$-number of J_d is the sum of the $s_{1,1}$-multiplicity and*

$$\sum_{j=0}^{\lfloor(\ell-4)/2\rfloor} \left(\frac{p+1}{2}\right)^2 \left(\frac{p-1}{2}\right)^{2j+1} \left(\frac{p^{\ell-3-2j}-1}{2}\right).$$

Proof. This follows from Proposition 5.9 using the multiplicities in Proposition 10.1. □

11. $J_d[p]$ in the Hermitian case

Suppose p is odd. Fix an integer $\lambda \geq 1$ and let $d = p^\lambda + 1$. In this case, the Fermat curve of degree d is isomorphic (over $\overline{\mathbb{F}}_p$) to the Hermitian curve H_q with equation $y_1^{q+1} = x_1^q + x_1$ where $q = p^\lambda$. It is well known that H_q is supersingular and its Ekedahl–Oort type was studied in [PW15]. Since C_d is a quotient of H_q, it is also supersingular in this case.

11.1. p-adic digits. Let $S = \mathbb{Z}/d\mathbb{Z} \setminus \{0, d/2\}$. Let $\pi : S \to S$ be induced by multiplication by p. Let $S_v = \{b \in S \mid 0 < b < d/2\}$ and $S_f = \{b \in S \mid d/2 < b < d\}$. Let

$$S' = \{(b_1, \ldots, b_\lambda) \mid 0 \leq b_j \leq p-1 \text{ and not all } b_j = (p-1)/2\}.$$

There is a bijection $S' \to S$ given by

$$(b_1, \ldots, b_\lambda) \mapsto b = 1 + \sum_{j=1}^{\lambda} b_j p^{j-1}.$$

Under this bijection, the permutation π is given by

$$(b_1, \ldots, b_\lambda) \mapsto (p-1-b_\lambda, b_1, \ldots, b_{\lambda-1}).$$

An element b belongs to S_v if and only if $b < (p^\lambda + 1)/2$. This is true if and only if, in the tuple, the entry b_j with largest j such that $b_j \neq (p-1)/2$ has the property that $b_j < (p-1)/2$.

11.2. Multiplicities. The multiplicative order of p modulo d is $\ell = 2\lambda$. We define a map $\mathrm{Pat}' : S \to \mathcal{W}_\lambda$ as follows: Given $b \in S$, the *pattern* $\mathrm{Pat}'(b)$ of b is the word $w = u_{\lambda-1} \cdots u_0$ given by

$$u_j = f \text{ if } p^j b \in S_f \text{ and } u_j = v \text{ if } p^j b \in S_v.$$

(The notation Pat' is used to distinguish this from the pattern in the encompassing case.) If the word for b has length ℓ (the maximum length), then it is $\mathrm{Pat}'(b)^c \cdot \mathrm{Pat}'(b)$ (where the c stands for the complementary word). For any $b \in S$, the word for b has a power with length ℓ and this power equals $\mathrm{Pat}'(b)^c \cdot \mathrm{Pat}'(b)$. Note that since $p^\lambda = -1 \pmod d$, the word of b is "self-dual", i.e., of the form $t^c t$, for every $b \in S$.

For a word w of length λ, let $\mu'(w)$ be the number of elements $b \in S$ with $\mathrm{Pat}'(b) = w$. For a word t of length $\le \lambda$, let $\mu'(\text{—}t)$ be the number of elements $b \in S$ with $\mathrm{Pat}'(b) = t' \cdot t$ for some t', in other words, the number of b with pattern ending in t.

Proposition 11.1. *Let p be odd.*

(1) *Suppose $e_1, \ldots, e_k$ are positive integers with $\sum e_i = \lambda$. If k is odd, then*

$$\mu'(f^{e_k} v^{e_{k-1}} \cdots f^{e_1}) = \mu'(v^{e_k} f^{e_{k-1}} \cdots v^{e_1}) = \left(\frac{p+1}{2}\right)^{\lambda-k} \left(\frac{p-1}{2}\right)^{k},$$

and if k is even, then

$$\mu'(v^{e_k} \cdots f^{e_1}) = \mu'(f^{e_k} \cdots v^{e_1}) = \left(\frac{p+1}{2}\right)^{\lambda+1-k} \left(\frac{p-1}{2}\right)^{k-1}.$$

(2) *More generally, given integers $e_1, \ldots, e_k > 0$, let $\lambda' = \sum e_i$ and suppose $\lambda' \le \lambda$. If k is odd, and t has the form $t = f^{e_k} v^{e_{k-1}} \cdots v^{e_2} f^{e_1}$, then*

$$\mu'(\text{—}t) = \mu'(\text{—}t^c) = \left(\frac{p+1}{2}\right)^{\lambda'-k} \left(\frac{p-1}{2}\right)^{k-1} \left(\frac{p^{\lambda+1-\lambda'} - 1}{2}\right),$$

and if k is even, and t has the form $t = v^{e_k} \cdots f^{e_1}$, then

$$\mu'(\text{—}t) = \mu'(\text{—}t^c) = \left(\frac{p+1}{2}\right)^{\lambda'-k} \left(\frac{p-1}{2}\right)^{k-1} \left(\frac{p^{\lambda+1-\lambda'} + 1}{2}\right).$$

Part (1) of Proposition 11.1 contradicts [PW15, Lemma 4.3], which we believe is in error.

Proof. Part (1) follows from part (2), so we will prove the latter. It is clear that $\mu'(\text{—}t) = \mu'(\text{—}t^c)$.

Suppose k is odd and $t = f^{e_k} v^{e_{k-1}} \cdots v^{e_2} f^{e_1}$. Write $f^{e_k} \cdots f^{e_1} = u_{\lambda'-1} \cdots u_0$ with $u_j \in \{f, v\}$. Then $b \in S$ has pattern —t if and only if the p-adic digits

$(b_1,\dots,b_\lambda)$ satisfy, for $\lambda+1-\lambda'<j\le\lambda$,

$$\begin{cases} b_j \le (p-1)/2 & \text{if } u_{\lambda-j}=v \text{ and } j \text{ is not a break of } t,\\ b_j < (p-1)/2 & \text{if } u_{\lambda-j}=v \text{ and } j \text{ is a break of } t,\\ b_j \ge (p-1)/2 & \text{if } u_{\lambda-j}=f \text{ and } j \text{ is not a break of } t,\\ b_j > (p-1)/2 & \text{if } u_{\lambda-j}=f \text{ and } j \text{ is a break of } t, \end{cases} \tag{11.1}$$

and the number corresponding to the tuple $\beta=(b_1,\dots,b_{\lambda+1-\lambda'})$ is large, namely

$$p^{\lambda+1-\lambda'}+1 > 1+\sum_{j=1}^{\lambda+1-\lambda'} b_j p^{j-1} > (p^{\lambda+1-\lambda'}+1)/2.$$

So there are $(p^{\lambda+1-\lambda'}-1)/2$ choices for β. Taking the product with the number of possibilities for b_j for $\lambda+1-\lambda'<j\le\lambda$ yields the quantity in the statement.

Similarly, if k is even and $t=v^{e_k}\cdots f^{e_1}=u_{\lambda'-1}\cdots u_0$ with $u_j\in\{f,v\}$, then $b\in S$ has pattern —t if and only if the p-adic digits $(b_1,\dots,b_\lambda)$ satisfy (11.1), for $\lambda+1-\lambda'<j\le\lambda$ and the number corresponding to the tuple β is small, namely

$$0<1+\sum_{j=1}^{\lambda+1-\lambda'} b_j p^{j-1} \le (p^{\lambda+1-\lambda'}+1)/2.$$

So there are $(p^{\lambda+1-\lambda'}+1)/2$ choices for β. Again, taking the product with the number of possibilities for b_j for $\lambda+1-\lambda'<j\le\lambda$ yields the quantity in the statement. □

Theorem 11.2. *Let p be odd and $d=p^\lambda+1$. Let $\mathcal{C}_d$ be the curve $y^d=x(1-x)$ and let J_d be its Jacobian. Then the Ekedahl–Oort type of J_d has the form $[\to^{\mu'_0}]$ if $\lambda=1$ and*

$$[\to^{\mu'_0}\nearrow^{\mu'_1}\cdots\nearrow^{\mu'_{2^{\lambda-1}-1}}]$$

if $\lambda>1$, where, letting $k(i)$ be the function described in Lemma 9.6,

$$\mu'_i=\begin{cases}\left(\frac{p+1}{2}\right)^{\lambda-k(i)-1}\left(\frac{p-1}{2}\right)^{k(i)+1} & \text{if } i \text{ is even},\\ \left(\frac{p+1}{2}\right)^{\lambda-k(i)}\left(\frac{p-1}{2}\right)^{k(i)} & \text{if } i \text{ is odd}.\end{cases}$$

Proof. This follows immediately from Theorem 7.1, the multiplicities in Proposition 11.1, and the number of breaks in Lemma 9.6. (Note that the k in Proposition 11.1 for w_i is $k(i)+1$.) □

11.3. Examples. Let p be odd.

(1) If $\lambda = 1$, the curve $\mathcal{C}_d$ has genus $(p-1)/2$ and is superspecial: the list of words starting with f and with positive multiplicity is fv, and the elementary sequence is
$$[\rightarrow^{(p-1)/2}] = [0, \ldots, 0].$$

(2) If $\lambda = 2$, the list of words is $ffvv$, $fvvf$, and the elementary sequence has a constant section of length $(p^2-1)/4$ and an increasing section of length $(p^2-1)/4$:
$$[\rightarrow^{(p^2-1)/4} \nearrow^{(p^2-1)/4}] = [0, \ldots, 0, 1, 2, \ldots, (p^2-1)/4].$$

(3) If $\lambda = 3$, the list of words is $f^3v^3, f^2v^3f, (fv)^3, fv^3f^2$, and the elementary sequence has four segments and has the form
$$[\rightarrow^m \nearrow^m \rightarrow^n \nearrow^m],$$
where $m = (p+1)^2(p-1)/8$ and $n = (p-1)^3/8$.

Proposition 11.3. *Let p be odd, let λ be a positive integer, and let $d = p^\lambda + 1$. Then:*

(1) *the p-rank of $J_d[p]$ is 0;*
(2) *the a-number of $J_d[p]$ is $(p-1)(p^{\lambda-1}+1)/4$;*
(3) *the $s_{1,1}$-multiplicity of $J_d[p]$ is 0 if λ is even and $(\frac{p-1}{2})^\lambda$ if λ is odd;*
(4) *and the $u_{1,1}$-number of $J_d[p]$ is the sum of the $s_{1,1}$-multiplicity and*

$$\sum_{j=0}^{\lfloor(\lambda-4)/2\rfloor} \left(\frac{p+1}{2}\right)^2 \left(\frac{p-1}{2}\right)^{2j+1} \left(\frac{p^{\lambda-3-2j}+1}{2}\right) + \begin{cases} 0 & \text{if } \lambda = 1, \\ \left(\frac{p+1}{2}\right)^2 \left(\frac{p-1}{2}\right)^{\lambda-2} & \text{if } \lambda > 1 \text{ and odd,} \\ \left(\frac{p+1}{2}\right) \left(\frac{p-1}{2}\right)^{\lambda-1} & \text{if } \lambda \text{ even.} \end{cases}$$

The analogue of the a-number calculation in part (2) for the Fermat curve of degree $d = p^\lambda + 1$ is given in [Gro90, Prop. 14.10].

Proof. This follows from Proposition 5.9 using the multiplicities in Proposition 11.1.

□

References

[AP15] Achter, Jeffrey. D.; Pries, Rachel. Superspecial rank of supersingular abelian varieties and Jacobians. *J. Théor. Nombres Bordeaux* **27** (2015), no. 13, 605–624. MR3429322, Zbl 1397.11100, doi: 10.5802/jtnb.916. 722, 728

[DH] Devalaparkur, Sanath; Halliday, John. The Dieudonné modules and Ekedahl–Oort types of Jacobians of hyperelliptic curves in odd characteristic. Preprint, 2017. arXiv:1712.04921. 706

[EP13] Elkin, Arsen; Pries, Rachel. Ekedahl–Oort strata of hyperelliptic curves in characteristic 2. *Algebra Number Theory* **7** (2013), no. 3, 507–532. MR3095219, Zbl 1282.11065, arXiv:1007.1226, doi: 10.2140/ant.2013.7.507. 706, 728

[Fon77] Fontaine, Jean-Marc. Groupes p-divisibles sur les corps locaux. Astérisque, No. 47-48. *Société Mathématique de France, Paris*, 1977. i+262 pp. MR0498610 (58 #16699), Zbl 0377.14009. 707

[Gon97] González, Josep. Hasse–Witt matrices for the Fermat curves of prime degree. *Tohoku Math. J. (2)* **49** (1997), no. 2, 149–163. MR1447179 (98b:11064), Zbl 0894.14010, doi: 10.2748/tmj/1178225144. 706, 730

[Gro90] Gross, Benedict H. Group representations and lattices. *J. Amer. Math. Soc.* **3** (1990), no. 4, 929–960. MR1071117 (92a:11077), Zbl 0745.11035, doi: 10.1090/S0894-0347-1990-1071117-8. 737

[Ill85] Illusie, Luc. Déformations de groupes de Barsotti–Tate (d'après A. Grothendieck). Seminar on arithmetic bundles: the Mordell conjecture (Paris, 1983/84). Astérisque, No. 127 (1985) 151–198. MR0801922, Zbl 1182.14050. 708

[KoW88] Kodama, Tetsuo; Washio, Tadashi. Hasse–Witt matrices of Fermat curves. *Manuscripta Math.* **60** (1988), no. 2, 185–195. MR0924086 (89b:14042), Zbl 0653.14014, doi: doi.org/10.1007/BF01161928. 706, 729

[Kra] Kraft, Hanspeter. Kommutative algebraische p-Gruppen (mit anwendungen auf p-divisible Gruppen und abelsche Varietäten). Sonderforschungsbereich, Universität Bonn, 1975. Manuscript, 86 pp. 709, 710

[LMPT19] Li, Wanlin; Mantovan, Elena; Pries, Rachel; Tang, Yunqing. Newton polygons arising from special families of cyclic covers of the projective line. *Res. Number Theory* **5** (2019), no. 1, Paper No. 12, 31 pp. MR3897613, Zbl 07086426, doi: 10.1007/s40993-018-0149-3 734

[MonS18] Montanucci, Maria; Speziali, Pietro. The a-numbers of Fermat and Hurwitz curves. *J. Pure Appl. Algebra* **222** (2018), no. 2, 477–488. MR3694465, Zbl 1427.11059, arXiv:1603.03604, doi: 10.1016/j.jpaa.2017.04.014. 706, 729

[Moo01] Moonen, Ben. Group schemes with additional structures and Weyl group cosets. *Moduli of abelian varieties*, (Texel Island, 1999), 255–298. Progr. Math., 195, *Birkhäuser, Basel*, 2001. MR1827024 (2002c:14074), Zbl 1084.14523, doi: 10.1007/978-3-0348-8303-0_10. 709, 713

[Moo04] Moonen, Ben. Serre–Tate theory for moduli spaces of PEL type. *Ann. Sci. École Norm. Sup. (4)* **37** (2004), no. 2, 223–269. MR2061781 (2005e:11075), Zbl 1107.11028, doi: 10.1016/j.ansens.2003.04.004. 706, 726

[Moo20] Moonen, Ben. Computing discrete invariants of varieties in positive characteristic I: Ekedahl–Oort types of curves. Preprint, 2020. https://www.math.ru.nl/ bmoonen/Papers/CDIPart1.pdf 706

[Oda69] Oda, Tadao. The first de Rham cohomology group and Dieudonné modules. *Ann. Sci. École Norm. Sup. (4)* **2** (1969), 63–135. MR0241435 (39 #2775), Zbl 0175.47901, doi: 10.24033/asens.1175. 706, 723

[Oor01] Oort, Frans. A stratification of a moduli space of abelian varieties. *Moduli of abelian varieties* (Texel Island, 1999), 345–416. Progr. Math., 195. *Birkhäuser, Basel*, 2001. MR1827027 (2002b:14055), Zbl 1052.14047, doi: 10.1007/978-3-0348-8303-0_13. 709, 711, 713, 714, 718

[PU] Pries, Rachel; Ulmer, Douglas. Every BT_1 group scheme appears in a Jacobian. Preprint, 2021. arXiv:2101.07946. 706, 707, 725, 726

[PW15] Pries, Rachel; Weir, Colin. The Ekedahl-Oort type of Jacobians of Hermitian curves. *Asian J. Math.* **19** (2015), no. 5, 845–869. MR3431681, Zbl 1392.11038, arXiv:1302.6261,doi: 10.4310/AJM.2015.v19.n5.a3. 706, 734, 735

[Sub75] Subrao, Doré. The p-rank of Artin–Schreier curves. *Manuscripta Math.* **16** (1975), no. 2, 169–193. MR0376693 (51 #12868), Zbl 0321.14017, doi: 10.1007/BF01181639. 728

[Ulm91] Ulmer, Douglas. p-descent in characteristic p. *Duke Math. J.* **62** (1991), no. 2, 237– 265. MR1104524 (92i:11068), Zbl 0742.14028, doi: 10.1215/S0012-7094-91-06210-1. 720, 722

[Ulm19] Ulmer, Douglas. On the Brauer-Siegel ratio for abelian varieties over function fields. *Algebra Number Theory* **13** (2019), no. 5, 1069–1120. MR3981314, Zbl 07083102, doi: 10.2140/ant.2019.13.1069. 723

[vdG99] van der Geer, Gerard. Cycles on the moduli space of abelian varieties. *Moduli of curves and abelian varieties*, 65–89. Aspects Math., E33, *Friedr. Vieweg, Braunschweig*, 1999. MR1722539 (2001b:14009), Zbl 0974.14031, arXiv:alg-geom/9605011, doi: 10.1007/978-3-322-90172-9_4. 709

[Yui80] Yui, Noriko. On the Jacobian variety of the Fermat curve. *J. Algebra* **65** (1980), no. 1, 1–35. MR0578793 (82m:14016), Zbl 0437.14015, doi: 10.1016/0021-8693(80)90236-7. 706, 730

(Rachel Pries) Department of Mathematics, Colorado State University, Fort Collins, CO 80523, USA
pries@math.colostate.edu

(Douglas Ulmer) Department of Mathematics, University of Arizona, Tucson, AZ 85721, USA
ulmer@math.arizona.edu

This paper is available via http://nyjm.albany.edu/j/2021/27-27.html.