JOURNAL
de Théorie des Nombres
de BORDEAUX
*anciennement Séminaire de Théorie des Nombres de Bordeaux*

Jeffrey D. ACHTER et Rachel PRIES

**Superspecial rank of supersingular abelian varieties and Jacobians**

Tome 27, n° 3 (2015), p. 605-624.

<http://jtnb.cedram.org/item?id=JTNB_2015__27_3_605_0>

*Journal de Théorie des Nombres*
*de Bordeaux* **27** (2015), 605–624

# Superspecial rank of supersingular abelian varieties and Jacobians

par Jeffrey D. ACHTER et Rachel PRIES

Résumé. Une variété abélienne définie sur un corps $k$ algébriquement clos de caractéristique positive est supersingulière si elle est isogène à un produit de courbes elliptiques supersingulières et est superspéciale si elle est isomorphe à un produit de courbes elliptiques supersingulières. Dans cet article, la condition d'être superspéciale est généralisée en définissant le *rang superspécial* d'une variété abélienne, qui est un invariant de sa $p$-torsion. Les principaux résultats de cet article concernent le rang superspécial des variétés abéliennes et des jacobiennes de courbes supersingulières. Il s'avère par exemple que le rang superspécial donne des informations sur la décomposition d'une variété abélienne à isomorphisme près; plus précisément celui-ci est une limite supérieure pour le nombre maximal de courbes elliptiques supersingulières apparaissant dans une telle décomposition.

Abstract. An abelian variety defined over an algebraically closed field $k$ of positive characteristic is supersingular if it is isogenous to a product of supersingular elliptic curves and is superspecial if it is isomorphic to a product of supersingular elliptic curves. In this paper, the superspecial condition is generalized by defining the *superspecial rank* of an abelian variety, which is an invariant of its $p$-torsion. The main results in this paper are about the superspecial rank of supersingular abelian varieties and Jacobians of curves. For example, it turns out that the superspecial rank determines information about the decomposition of a supersingular abelian variety up to isomorphism; namely it is a bound for the maximal number of supersingular elliptic curves appearing in such a decomposition.

## 1. Introduction

If $A$ is a principally polarized abelian variety of dimension $g$ defined over an algebraically closed field $k$ of positive characteristic $p$, then the

Manuscrit reçu le 19 février 2014, révisé le 8 septembre 2015, accepté le 2 octobre 2015.
*Mathematics Subject Classification.* 11G10, 11G20, 14F40, 14H40, 14L15.
*Mots-clefs.* abelian variety, Jacobian, supersingular, superspecial, $p$-torsion, Dieudonné module.

multiplication-by-$p$ morphism $[p] = \mathrm{Ver} \circ \mathrm{Fr}$ is inseparable. Typically, $A$ is *ordinary* in that the Verschiebung morphism Ver is separable, a condition equivalent to the number of $p$-torsion points of $A$ being $p^g$, or the only slopes of the $p$-divisible group of $A$ being 0 and 1, or the $p$-torsion group scheme of $A$ being isomorphic to $(\mathbb{Z}/p \oplus \boldsymbol{\mu}_p)^g$.

Yet the abelian varieties which capture great interest are those which are as far from being ordinary as possible. In dimension $g = 1$, an elliptic curve is *supersingular* if it has no points of order $p$; if the only slope of its $p$-divisible group is $1/2$; or if its $p$-torsion group scheme is isomorphic to the unique local-local $\mathrm{BT}_1$ group scheme of rank $p^2$, which we denote by $I_{1,1}$.

These characterizations are different for a principally polarized abelian variety $A$ of higher dimension $g$. One says that $A$ has *$p$-rank* 0 when $A$ has no points of order $p$; that $A$ is *supersingular* when the only slope of its $p$-divisible group is $1/2$; and that $A$ is *superspecial* when its $p$-torsion group scheme is isomorphic to $I_{1,1}^g$. If $A$ is supersingular, then it has $p$-rank 0, but the converse is false for $g \geq 3$. If $A$ is superspecial, then it is supersingular, but the converse is false for $g \geq 2$.

The Newton polygon and Ekedahl-Oort type of an abelian variety usually do not determine the decomposition of the abelian variety. In fact, for any prime $p$ and formal isogeny type $\eta$ other than the supersingular one, there exists an absolutely simple abelian variety over $k$ having Newton polygon $\eta$ [15]. On the other hand, consider the following results about supersingular and superspecial abelian varieties.

**Theorem 1.1** (Oort)**.** *Let $A/k$ be a principally polarized abelian variety.*

(1) *Then $A$ is supersingular if and only if it is isogenous to a product of supersingular elliptic curves by* [24, Theorem 4.2] *(which uses* [35, Theorem 2d]*).*
(2) *Then $A$ is superspecial if and only if it is isomorphic to a product of supersingular elliptic curves* [25, Theorem 2]*, see also* [20, Theorem 4.1]*.*

The motivation for this paper was to find ways to measure the extent to which supersingular non-superspecial abelian varieties decompose up to isomorphism. The $a$-number $a := \dim_k \mathrm{Hom}(\boldsymbol{\alpha}_p, A[p])$ gives some information about this; if $A$ has $p$-rank 0, then the number of factors in the decomposition of $A$ up to isomorphism is bounded above by the $a$-number, see [7, Lemma 5.2]. However, a supersingular abelian variety with large $a$-number could still be indecomposable up to isomorphism.

This paper is about another invariant of $A$, the *superspecial rank*, which we define in Section 3.2 as the number of (polarized) factors of $I_{1,1}$ appearing in the $p$-torsion group scheme of $A$. In Proposition 3.12, we determine which superspecial ranks occur for supersingular abelian varieties.

The superspecial rank of Jacobians also has an application involving Selmer groups, see Section 3.5.

In Section 4, we define another invariant of $A$, the *elliptic rank*, which is the maximum number of elliptic curves appearing in a decomposition of $A$ up to isomorphism. In Proposition 4.4, we prove an observation of Oort which states that, for a supersingular abelian variety $A$, the elliptic rank equals the number of rank 2 factors in the $p$-divisible group $A[p^\infty]$. Proposition 4.2 states that the elliptic rank is bounded by the superspecial rank for an abelian variety of $p$-rank 0. As a result, for an abelian variety $A$ of $p$-rank zero, the superspecial rank gives an upper bound for the maximal number of dimension one factors in a decomposition of $A$ up to isomorphism; this upper bound is most interesting for supersingular abelian varieties, which decompose completely up to isogeny.

In Section 5, we apply this observation to prove some results about the superspecial rank and elliptic rank of Jacobians of curves. For example, in characteristic 2, Application 5.5 states that the superspecial rank of the Jacobian of any hyperelliptic curve of 2-rank $r$ is bounded by $1 + r$, while its elliptic rank is bounded by $1 + 2r$. The superspecial ranks of all the Hermitian curves are computed in Section 5.3; in particular, when $n$ is even the elliptic rank of the Hermitian curve $X_{p^n}$ is zero.

**Acknowledgment.** The authors thank the organizers of the 2013 Journées Arithmétiques, the referee for valuable comments, Ritzenthaler for help with the French abstract, and Oort for sharing the idea for Proposition 4.4 and more generally for being a source of inspiration for this work. The first-named author was partially supported by grants from the Simons Foundation (204164) and the NSA (H98230-14-1-0161 and H98230-15-1-0247). The second-named author was partially supported by NSF grants DMS-11-01712 and DMS-15-02227.

## 2. Notation

All geometric objects in this paper are defined over an algebraically closed field $k$ of characteristic $p > 0$. Some objects are defined over the ring $W(k)$ of Witt vectors over $k$. Let $\sigma$ denote the Frobenius automorphism of $k$ and its lift to $W(k)$. Let $A$ be a principally polarized abelian variety of dimension $g$ over $k$. Here are some relevant facts about $p$-divisible groups and $p$-torsion group schemes.

**2.1. The $p$-divisible group.** By the Dieudonné-Manin classification [18], there is an isogeny of $p$-divisible groups

$$A[p^\infty] \sim \oplus_{\lambda=\frac{d}{c+d}} \widetilde{G}_{c,d}^{m_\lambda},$$

where $(c,d)$ ranges over pairs of relatively prime nonnegative integers, and $\widetilde{G}_{c,d}$ denotes a $p$-divisible group of codimension $c$, dimension $d$, and thus height $c+d$. The Dieudonné module $\widetilde{D}_\lambda := \mathbb{D}_*(\widetilde{G}_{c,d})$ (see 2.3 below) is a free $W(k)$-module of rank $c+d$. Over $\operatorname{Frac} W(k)$, there is a basis $x_1, \dots, x_{c+d}$ for $\widetilde{D}_\lambda$ such that $F^d x_i = p^c x_i$. The Newton polygon of $A$ is the data of the numbers $m_\lambda$; it admits an intepretation as the $p$-adic Newton polygon of the operator $F$ on $\mathbb{D}_*(A[p^\infty])$.

The abelian variety $A$ is *supersingular* if and only if $\lambda = \frac{1}{2}$ is the only slope of its $p$-divisible group $A[p^\infty]$. Letting $\widetilde{I}_{1,1} = \widetilde{G}_{1,1}$ denote the $p$-divisible group of dimension 1 and height 2, one sees that $A$ is supersingular if and only $A[p^\infty] \sim \widetilde{I}_{1,1}^g$.

**2.2. The $p$-torsion group scheme.** The multiplication-by-$p$ morphism $[p] : A \to A$ is a finite flat morphism of degree $p^{2g}$. The *$p$-torsion group scheme* of $A$ is

$$A[p] = \operatorname{Ker}[p] = \operatorname{Ker}(\operatorname{Ver} \circ \operatorname{Fr}),$$

where $\operatorname{Fr} : A \to A^{(p)}$ denotes the relative Frobenius morphism and $\operatorname{Ver} : A^{(p)} \to A$ is the Verschiebung morphism. In fact, $A[p]$ is a $\mathrm{BT}_1$ group scheme as defined in [26, 2.1, Definition 9.2]; it is killed by $[p]$, with $\operatorname{Ker}(\operatorname{Fr}) = \operatorname{Im}(\operatorname{Ver})$ and $\operatorname{Ker}(\operatorname{Ver}) = \operatorname{Im}(\operatorname{Fr})$.

The principal polarization on $A$ induces a principal quasipolarization on $A[p]$, i.e., an anti-symmetric isomorphism $\psi : A[p] \to A[p]^D$. (This definition must be modified slightly if $p = 2$.) Summarizing, $A[p]$ is a principally quasipolarized (pqp) $\mathrm{BT}_1$ group scheme of rank $p^{2g}$.

Isomorphisms classes of pqp $\mathrm{BT}_1$ group schemes over $k$ (also known as Ekedahl-Oort types) have been completely classified [26, Theorem 9.4 & 12.3], building on unpublished work of Kraft [14] (which did not include polarizations) and of Moonen [19] (for $p \geq 3$). (When $p = 2$, there are complications with the polarization which are resolved in [26, 9.2, 9.5, 12.2].)

**2.3. Covariant Dieudonné modules.** The $p$-divisible group $A[p^\infty]$ and the $p$-torsion group scheme $A[p]$ can be described using covariant Dieudonné theory; see e.g., [26, 15.3]. Briefly, let $\widetilde{\mathbb{E}} = \widetilde{\mathbb{E}}(k) = W(k)[F,V]$ denote the non-commutative ring generated by semilinear operators $F$ and $V$ with relations

$$FV = VF = p,\ F\lambda = \lambda^\sigma F,\ \lambda V = V\lambda^\sigma, \tag{2.1}$$

for all $\lambda \in W(k)$. There is an equivalence of categories $\mathbb{D}_*$ between $p$-divisible groups over $k$ and $\widetilde{\mathbb{E}}$-modules which are free of finite rank over $W(k)$.

Similarly, let $\mathbb{E} = \widetilde{\mathbb{E}} \otimes_{W(k)} k$ be the reduction of the Cartier ring mod $p$; it is a non-commutative ring $k[F,V]$ subject to the same constraints as (2.1), except that $FV = VF = 0$ in $\mathbb{E}$. Again, there is an equivalence of categories

$\mathbb{D}_*$ between finite commutative group schemes (of rank $2g$) annihilated by $p$ and $\mathbb{E}$-modules of finite dimension $(2g)$ over $k$. If $M = \mathbb{D}_*(G)$ is the Dieudonné module over $k$ of $G$, then a principal quasipolarization $\psi : G \to G^D$ induces a a nondegenerate symplectic form

$$\langle \cdot, \cdot \rangle : M \times M \longrightarrow k \tag{2.2}$$

on the underlying $k$-vector space of $M$, subject to the additional constraint that, for all $x$ and $y$ in $M$,

$$\langle Fx, y \rangle = \langle x, Vy \rangle^\sigma. \tag{2.3}$$

If $A$ is the Jacobian of a curve $X$, then there is an isomorphism of $\mathbb{E}$-modules between the *contravariant* Dieudonné module over $k$ of $\mathrm{Jac}(X)[p]$ and the de Rham cohomology group $H^1_{\mathrm{dR}}(X)$ by [21, Section 5]. The canonical principal polarization on $\mathrm{Jac}(X)$ then induces a canonical isomorphism $\mathbb{D}_*(\mathrm{Jac}(X)[p]) \simeq H^1_{\mathrm{dR}}(X)$; we will use this identification without further comment.

For elements $A_1, \ldots, A_r \in \mathbb{E}$, let $\mathbb{E}(A_1, \ldots, A_r)$ denote the left ideal $\sum_{i=1}^r \mathbb{E}A_i$ of $\mathbb{E}$ generated by $\{A_i \mid 1 \le i \le r\}$.

**2.4. The *p*-rank and *a*-number.** For a $\mathrm{BT}_1$ group scheme $G/k$, the *p-rank* of $G$ is $f = \dim_{\mathbb{F}_p}\mathrm{Hom}(\boldsymbol{\mu}_p, G)$ where $\boldsymbol{\mu}_p$ is the kernel of Frobenius on $\mathbb{G}_m$. Then $p^f$ is the cardinality of $G(k)$. The *a-number* of $G$ is

$$a = \dim_k \mathrm{Hom}(\boldsymbol{\alpha}_p, G),$$

where $\boldsymbol{\alpha}_p$ is the kernel of Frobenius on $\mathbb{G}_a$. It is well-known that $0 \le f \le g$ and $1 \le a + f \le g$.

Moreover, since $\boldsymbol{\mu}_p$ and $\boldsymbol{\alpha}_p$ are both simple group schemes, the $p$-rank and $a$-number are additive;

$$f(G \oplus H) = f(G) + f(H) \text{ and } a(G \oplus H) = a(G) + a(H). \tag{2.4}$$

If $\widetilde{G}$ is a $p$-divisible group, its $p$-rank and $a$-number are those of its $p$-torsion; $f(\widetilde{G}) = f(\widetilde{G}[p])$ and $a(\widetilde{G}) = a(\widetilde{G}[p])$. Similarly, if $A$ is an abelian variety, then $f(A) = f(A[p])$ and $a(A) = a(A[p])$.

**2.5. The Ekedahl-Oort type.** As in [26, Sections 5 & 9], the isomorphism type of a pqp $\mathrm{BT}_1$ group scheme $G$ over $k$ can be encapsulated into combinatorial data. If $G$ is symmetric with rank $p^{2g}$, then there is a *final filtration* $N_1 \subset N_2 \subset \cdots \subset N_{2g}$ of $\mathbb{D}_*(G)$ as a $k$-vector space which is stable under the action of $V$ and $F^{-1}$ such that $i = \dim(N_i)$ [26, 5.4].

The *Ekedahl-Oort type* of $G$ is

$$\nu = [\nu_1, \ldots, \nu_g], \text{ where } \nu_i = \dim(V(N_i)).$$

The $p$-rank is $\max\{i \mid \nu_i = i\}$ and the $a$-number equals $g - \nu_g$. There is a restriction $\nu_i \le \nu_{i+1} \le \nu_i + 1$ on the Ekedahl-Oort type. There are $2^g$ Ekedahl-Oort types of length $g$ since all sequences satisfying this restriction

occur. By [26, 9.4, 12.3], there are bijections between (i) Ekedahl-Oort types of length $g$; (ii) pqp $\mathrm{BT}_1$ group schemes over $k$ of rank $p^{2g}$; and (iii) pqp Dieudonné modules of dimension $2g$ over $k$.

**Example 2.1.** *The group scheme $I_{1,1}$.* There is a unique $\mathrm{BT}_1$ group scheme of rank $p^2$ which has $p$-rank 0, which we denote $I_{1,1}$. It fits in a non-split exact sequence

$$0 \to \boldsymbol{\alpha}_p \to I_{1,1} \to \boldsymbol{\alpha}_p \to 0. \tag{2.5}$$

The structure of $I_{1,1}$ is uniquely determined over $\overline{\mathbb{F}}_p$ by this exact sequence. The image of $\boldsymbol{\alpha}_p$ is the kernel of Fr and Ver. The Dieudonné module of $I_{1,1}$ is

$$M_{1,1} := \mathbb{D}_*(I_{1,1}) \simeq \mathbb{E}/\mathbb{E}(F+V).$$

If $E$ is a supersingular elliptic curve, then the $p$-torsion group scheme $E[p]$ is isomorphic to $I_{1,1}$.

## 3. Superspecial rank

Let $A$ be a principally polarized abelian variety defined over an algebraically closed field $k$ of characteristic $p > 0$.

**3.1. Superspecial.** First, recall the definition of the superspecial property.

**Definition 3.1.** One says that $A/k$ is *superspecial* if it satisfies the following equivalent conditions:

(1) The $a$-number of $A$ equals $g$.
(2) The group scheme $A[p]$ is isomorphic to $I_{1,1}^g$.
(3) The Dieudonné module over $k$ of $A[p]$ is isomorphic to $M_{1,1}^g$.
(4) $A$ is isomorphic (as an abelian variety without polarization) to the product of $g$ supersingular elliptic curves.

A superspecial abelian variety is defined over $\overline{\mathbb{F}}_p$, and thus over a finite field. For every $g \in \mathbb{N}$ and prime $p$, the number of superspecial principally polarized abelian varieties of dimension $g$ defined over $\overline{\mathbb{F}}_p$ is finite and nonzero.

**3.2. Definition of superspecial rank.** Recall (Example 2.1) that the $p$-torsion group scheme of a supersingular elliptic curve is isomorphic to $I_{1,1}$, the unique local-local pqp $\mathrm{BT}_1$ group scheme of rank $p^2$. From (2.5), it follows that $I_{1,1}$ is not simple as a group scheme. However, $I_{1,1}$ is simple in the category of $\mathrm{BT}_1$ group schemes since $\boldsymbol{\alpha}_p$ is not a $\mathrm{BT}_1$ group scheme.

**Definition 3.2.** Let $G/k$ be a $\mathrm{BT}_1$ group scheme. A *superspecial factor* of $G$ is a group scheme $H \subset G$ with $H \simeq I_{1,1}^s$.

By the equivalence of categories $\mathbb{D}_*$, superspecial factors of $G$ of rank $2s$ are in bijection with $\mathbb{E}$-submodules $N \subset \mathbb{D}_*(G)$ with $N \simeq (\mathbb{E}/\mathbb{E}(F+V))^s$; we call such an $N$ a *superspecial factor* of $M = \mathbb{D}_*(G)$.

Now suppose $(G,\psi)/k$ is a pqp $\mathrm{BT}_1$ group scheme. A superspecial factor $H$ of $G$ is *polarized* if the isomorphism $\psi : G \to G^D$ restricts to an isomorphism $\psi_H : H \to G^D \twoheadrightarrow H^D$. Equivalently, a superspecial factor $N$ of $(\mathbb{D}_*(G), \langle\cdot,\cdot\rangle)$ is polarized if the nondegenerate symplectic form $\langle\cdot,\cdot\rangle : M\times M \to k$ restricts to a non-degenerate symplectic form $\langle\cdot,\cdot\rangle : N\times N \to k$.

**Definition 3.3.** Let $G = (G,\psi)/k$ be a pqp $\mathrm{BT}_1$ group scheme. The *superspecial rank* $s(G)$ of $G$ is the largest integer $s$ for which $G$ has a polarized superspecial factor of rank $2s$.

Since $I_{1,1}$ is simple in the category of $\mathrm{BT}_1$ group schemes, the superspecial rank $s$ has an additive property similar to that for the $p$-rank and $a$-number (2.4); if $G$ and $H$ are pqp $\mathrm{BT}_1$ group schemes, then

$$s(G\oplus H) = s(G) + s(H). \tag{3.1}$$

A $\mathrm{BT}_1$ group scheme $G$ may fail to be simple (i.e., admit a nontrivial $\mathrm{BT}_1$ subgroup scheme $0 \subsetneq H \subsetneq G$) and yet still be indecomposable (i.e., admit no isomorphism $G \simeq H\oplus K$ with $H$ and $K$ nonzero). This distinction vanishes in the category of pqp $\mathrm{BT}_1$ group schemes:

**Lemma 3.4.** *Let $G/k$ be a pqp $\mathrm{BT}_1$ group scheme, and let $H \subset G$ be a pqp $\mathrm{BT}_1$ sub-group scheme. Let $N = \mathbb{D}_*(H) \subseteq M = \mathbb{D}_*(G)$, and let $P$ be the orthogonal complement of $N$ in $M$. Then $P$ is a pqp sub-Dieudonné module of $M$, and $G$ admits a decomposition $G \simeq H \oplus K$ as pqp $\mathrm{BT}_1$ group schemes, where $K \subseteq G$ is the sub-group scheme with $\mathbb{D}_*(K) = P$.*

Lemma 3.4 is essentially present in [14, Section 5]; see, e.g., [26, 9.8].

*Proof.* The $k$-vector space $P$ is an $\mathbb{E}$-module if it is stable under $F$ and $V$. It suffices to check that, for $\beta \in P$, $F\beta \in P$ and $V\beta \in P$. If $\alpha \in N$, the relation (2.3) implies that

$$\langle F\beta, \alpha\rangle = \langle \beta, V\alpha\rangle^\sigma = 0^\sigma = 0$$

and

$$\langle V\beta, \alpha\rangle = \langle \beta, F\alpha\rangle^{\sigma^{-1}} = 0^{\sigma^{-1}} = 0.$$

Thus $F\beta$ and $V\beta$ are in the orthogonal complement $P$ of $N$.

Since $H$ is polarized, the restriction of $\langle\cdot,\cdot\rangle$ to $N$ is perfect and so the restriction of $\langle\cdot,\cdot\rangle$ to $P$ is perfect as well. Since $\mathbb{D}_*$ is an equivalence of categories, there is a decomposition $G \simeq H \oplus K$ as pqp group schemes. It remains to verify that $K$ is a $\mathrm{BT}_1$ group scheme, i.e., that $\mathrm{Ker}(\mathrm{Fr}) = \mathrm{Im}(\mathrm{Ver})$ and $\mathrm{Ker}(\mathrm{Ver}) = \mathrm{Im}(\mathrm{Fr})$. In terms of Dieudonné modules, this is equivalent to the property that $\mathrm{Ker}\, F|_P = V(P)$ and $\mathrm{Ker}\, V|_P = F(P)$.

This, in turn, follows from the analogous statement for $M$ and $N$ and from the fact that the decomposition $M = N \oplus P$ is stable under $F$ and $V$. □

**Lemma 3.5.** *Let $G/k$ be a pqp $\mathrm{BT}_1$ group scheme of $p$-rank $f$ and $a$-number $a$, and let $H \subset G$ be a maximal polarized superspecial factor. Then $G \simeq H \oplus K$ for a pqp $\mathrm{BT}_1$ group scheme $K$ with respective $p$-rank, superspecial rank and $a$-number $f(K) = f$, $s(K) = 0$, and $a(K) = a - s$.*

*Proof.* The existence of the decomposition $G \simeq H \oplus K$ follows from Lemma 3.4; the assertions about the $p$-rank, superspecial rank and $a$-number of $K$ follow from the additivity of these quantities, (2.4) and (3.1). □

Since one can always canonically pull off the étale and toric components of a finite group scheme over a perfect field, Lemma 3.5 admits a further refinement:

**Lemma 3.6.** *Let $G/k$ be a pqp $\mathrm{BT}_1$ group scheme with $f(G) = f$, $s(G) = s$, and $a(G) = a$. Then there is a local-local pqp $\mathrm{BT}_1$ group scheme $B$ such that*

$$G \simeq (\mathbb{Z}/p \oplus \boldsymbol{\mu}_p)^f \oplus I_{1,1}^s \oplus B$$

*where $f(B) = s(B) = 0$ and $a(B) = a - s$.*

*Proof.* Since $k$ is perfect and $G$ is self-dual, there is a canonical decomposition of pqp group schemes $G \simeq (\mathbb{Z}/p \oplus \boldsymbol{\mu}_p)^f \oplus H$. Then $f(H) = 0$, $s(H) = s(G)$, and $a(H) = a(G)$. Now invoke Lemma 3.5. □

Let $A$ be a principally polarized abelian variety of dimension $g$. On one hand, $A$ is superspecial if and only if $s(A[p]) = g$. On the other hand, if $A$ is ordinary, then $s(A[p]) = 0$. More generally:

**Lemma 3.7.** *Let $G/k$ be a pqp $\mathrm{BT}_1$ group scheme of rank $p^{2g}$; let $f = f(G)$, $a = a(G)$, and $f = f(G)$.*

(a) *Then $0 \le s \le a \le g - f$.*
(b) *If $a = g - f$, then $G \simeq (\mathbb{Z}/p \oplus \boldsymbol{\mu}_p)^f \oplus I_{1,1}^a$ and $s = a$.*
(c) *If $a \ne g - f$, then $s < a$.*

*Proof.* Write $G \simeq (\mathbb{Z}/p \oplus \boldsymbol{\mu}_p)^f \oplus B_1$ with $B_1 \simeq I_{1,1}^s \oplus B$ as in Lemma 3.6.

(a) Then $a \le g - f$, since (using additivity) $a(G) = a(B_1)$, and $B_1$ has rank $p^{2(g-f)}$. Moreover, $s \le a$ since $a(I_{1,1}^s) = s$.
(b) This is true since the only pqp $\mathrm{BT}_1$ group scheme of rank $p^{2(g-f)}$ with $p$-rank 0 and $a$-number $g - f$ is $I_{1,1}^{g-f}$, which has superspecial rank $g - f$ by definition.
(c) The hypothesis $a \ne g - f$ implies that $B$ is non-trivial. Then $a > s$ since the $a$-number of the local-local group scheme $B$ is at least 1. □

**3.3. Unpolarized superspecial rank.** If $G/k$ is a $\mathrm{BT}_1$ group scheme, or indeed any $p$-torsion finite commutative group scheme, then there is also an obvious notion of an *unpolarized* superspecial rank, namely, the largest $u$ such that there is an inclusion $I_{1,1}^u \hookrightarrow G$. In this section, we briefly explore some of the limitations of this notion.

For integers $r, s \geq 1$, let $J_{r,s}$ be the $\mathrm{BT}_1$ group scheme with Dieudonné module

$$M_{r,s} := \mathbb{D}_*(J_{r,s}) = \mathbb{E}/\mathbb{E}(F^r + V^s).$$

**Lemma 3.8.** *Suppose $r, s \geq 2$. Then*

(a) *$J_{r,s}$ is an indecomposable local-local $\mathrm{BT}_1$ group scheme.*
(b) *There exists an inclusion $\iota : I_{1,1} \hookrightarrow J_{r,s}$.*

*Proof.* Part (a) is standard. Indeed, using the relations $F^r = -V^s$ and $FV = VF = p$, one sees that $F$ and $V$ act nilpotently, and thus $J_{r,s}$ is local-local; in particular, it has $p$-rank zero. Note that $M_{r,s}$ is generated over $\mathbb{E}$ by a single element $x$ such that $F^r x = -V^s x$. It follows that $a(J_{r,s}) = 1$. The additivity relation (2.4) now implies that $M_{r,s}$ is indecomposable.

For (b), let $y \in M_{r,s}$ be an element such that $Fy = -Vy \neq 0$. Since $r, s \geq 2$, the element $y = F^{r-1}x + V^{s-1}x$ is suitable. Then there is an inclusion $\iota_* : M_{1,1} \to M_{r,s}$ which sends a generator of $M_{1,1}$ to $y$. □

If $r = s$, then $J_{r,s}$ is self-dual and admits a principal quasipolarization; in this case, let $H_{r,s} = J_{r,s}$. If $r \neq s$, then the Cartier dual of $J_{r,s}$ is $J_{s,r}$; in this case, $H_{r,s} := J_{r,s} \oplus J_{s,r}$ admits a principal quasipolarization.

In spite of Lemma 3.8, we find:

**Lemma 3.9.** *Suppose $r, s \geq 2$. For any principal quasipolarization on $H_{r,s}$, the superspecial rank of $H_{r,s}$ is zero.*

*Proof.* If $r = s$, this is immediate, since $H_{r,r}$ is indecomposable by Lemma 3.8 and yet a polarized superspecial factor of positive rank would induce a factorization by Lemma 3.4.

Now suppose $r \neq s$. The argument used in the classification of polarizations on superspecial $p$-divisible groups in [17, Section 6.1] shows that for some $u \in \{1, 2\}$, there exists an inclusion $\iota : I_{1,1}^u \hookrightarrow H_{r,s}$ with $G := \iota(I_{1,1}^u)$ polarized. If $G$ is contained in either $J_{r,s}$ or $J_{s,r}$ (and in particular if $u = 1$), then we may argue as before. Otherwise, consider the sum of $G$ and $J_{r,s}$ inside $H_{r,s}$, which is *not* direct since $G \cap J_{r,s} \simeq I_{1,1}$ is nonempty. By Lemma 3.4, $G$ has a complement $K$ in $G + J_{r,s}$. Then $J_{r,s} \simeq I_{1,1} \oplus K$, contradicting the indecomposability of $J_{r,s}$. □

**3.4. Superspecial ranks of abelian varieties.** If $A/k$ is a principally polarized abelian variety, we define its superspecial rank to be that of its $p$-torsion group scheme; $s(A) = s(A[p])$. Lemma 3.7 gives constraints between

the $p$-rank, $a$-number, and superspecial rank of $A$. It turns out that these are the only constraints on $f$, $a$ and $s$:

**Proposition 3.10.** *Given integers $g, f, a, s$ such that $0 \leq s < a < g - f$, there exists a principally polarized abelian variety $A/k$ of dimension $g$ with $p$-rank $f$, $a$-number $a$ and superspecial rank $s$.*

*Proof.* By [26, Theorem 1.2], it suffices to show that there exists a pqp $\mathrm{BT}_1$ group scheme $G$ of rank $p^{2g}$ with $p$-rank $f$, $a$-number $a$ and superspecial rank $s$. Set

$$g_1 = g - f - s, \text{ and } a_1 = a - s,$$

and note that $a_1 \geq 1$ and $g_1 - a_1 \geq 1$ by hypothesis. Considering

$$G = (\mathbb{Z}/p \oplus \boldsymbol{\mu}_p)^f \oplus I_{1,1}^s \oplus B,$$

together with the product polarization, allows one to reduce to the case of finding a pqp $\mathrm{BT}_1$ group scheme $B$ of rank $p^{2g_1}$ with $p$-rank 0, $a$-number $a_1$ and superspecial rank 0. This is possible as follows.

Consider the word $w$ in $F$ and $V$ given by

$$w = F^{g_1 - a_1 + 1}(VF)^{a_1 - 1}V^{g_1 - a_1 + 1}.$$

Then $w$ is simple and symmetric with length $2g_1$, and thus the corresponding $\mathrm{BT}_1$ group scheme admits a canonical principal quasipolarization [26, 9.11]. Let $L_1, \ldots, L_{2g_1} \in \{F, V\}$ be such that $w = L_1 \cdots L_{2g_1}$. Consider variables $z_1, \ldots, z_{2g_1}$ with $z_{2g_1+1} = z_1$. As in [26, Section 9.8], the word $w$ defines the structure of a Dieudonné module on $N_w = \oplus_i k \cdot z_i$ as follows: if $L_i = F$, let $F(z_i) = z_{i+1}$ and $V(z_{i+1}) = 0$; if $L_i = V$, let $V(z_{i+1}) = z_i$ and $F(z_i) = 0$.

The $a$-number is the number of generators for $N_w$ as an $\mathbb{E}$-module. By construction, $N_w$ has $a$-number $a_1$. Since $g_1 - a_1 + 1 \geq 2$, then $N_w$ has superspecial rank 0. □

We now focus on supersingular abelian varieties

**Lemma 3.11.** *For every $g \geq 2$ and prime $p$, a generic supersingular principally polarized abelian variety of dimension $g$ over $k$ has superspecial rank 0.*

*Proof.* A generic supersingular principally polarized abelian variety has $p$-rank 0 and $a$-number 1 [17, Section 4.9]. This forces its Ekedahl-Oort type to be $[0, 1, \ldots, g-1]$, its Dieudonné module to be $M_{g,g}$, and its superspecial rank to be zero (Lemma 3.9) since $g \geq 2$. □

It is not difficult to classify the values of the supersingular rank which occur for supersingular abelian varieties.

**Proposition 3.12.** *For every $g \geq 2$ and prime $p$, there exists a supersingular principally polarized abelian variety of dimension $g$ over $k$ with superspecial rank $s$ if and only if $0 \leq s \leq g-2$ or $s = g$.*

*Proof.* It is impossible for the superspecial rank to be $g-1$ since there are no local-local pqp $\mathrm{BT}_1$ group schemes of rank $p^2$ other than $I_{1,1}$.

For the reverse implication, recall that there exists a supersingular principally polarized abelian variety $A_1/k$ of dimension $g-s$ with $a = 1$. Its Dieudonné module is $M_{g-s,g-s}$. In particular, $s(A_1) = 0$ as long as $s \leq g-2$ (Lemma 3.9). Let $E$ be a supersingular elliptic curve. Then $A = E^s \times A_1$, together with the product polarization, is a supersingular principally polarized abelian variety over $k$ with dimension $g$ and $s(A) = s$. □

**Example 3.13.** Let $A/k$ be a supersingular principally polarized abelian variety of dimension 3. Then the $a$-number $a = a(A)$ satisfies $1 \leq a \leq 3$.

(a) If $a = 1$, then $A[p] \simeq J_{3,3}$, which has superspecial rank $s = 0$.
(b) If $a = 2$, then $A[p^\infty] \simeq \widetilde{G}_{1,1} \times \widetilde{Z}$ where $\widetilde{Z}$ is supergeneral of height 4 and $a(\widetilde{Z}) = 1$ [22]. Then $s(\widetilde{Z}[p]) = 0$ (Lemma 3.7(c)) and thus $s(A) = 1$.
(c) If $a = 3$, then $A$ has superspecial rank $s = 3$.

**3.5. Application of superspecial rank to Selmer groups.** Here is another motivation for studying the superspecial rank of Jacobians. The superspecial rank equals the rank of the Selmer group associated with a particular isogeny of function fields in positive characteristic. Let $K$ be the function field of a smooth projective connected curve $X$ over $k$. Let $\mathcal{E}$ be a constant supersingular elliptic curve over $K$. Consider the multiplication-by-$p$ isogeny $f = [p] : \mathcal{E} \to \mathcal{E}$ of abelian varieties over $K$.

Recall the Tate-Shafarevich group

$$Ш(K, \mathcal{E})_f = \mathrm{Ker}(\, Ш(K, \mathcal{E}) \xrightarrow{f} Ш(K, \mathcal{E})),$$

where

$$Ш(K, \mathcal{E}) = \mathrm{Ker}(H^1(K, \mathcal{E}) \to \prod_v H^1(K_v, \mathcal{E}))$$

and $v$ runs over all places of $K$. The Selmer group $\mathrm{Sel}(K, f)$ is the subset of elements of $H^1(K, \mathrm{Ker}(f))$ whose restriction is in the image of

$$\mathrm{Sel}(K_v, f) = \mathrm{Im}(\mathcal{E}(K_v) \to H^1(K_v, \mathrm{Ker}(f))),$$

for all $v$. There is an exact sequence

$$0 \to \mathcal{E}(K)/f(\mathcal{E}(K)) \to \mathrm{Sel}(K, f) \to Ш(K, \mathcal{E})_f \to 0.$$

Here is an earlier result, rephrased using the terminology of this paper, which provides motivation for studying the superspecial rank.

**Theorem 3.14.** *(Ulmer) The rank of* $\mathrm{Sel}(K, [p])$ *is the superspecial rank of* $\mathrm{Jac}(X)$ [36, Proposition 4.3].

## 4. Elliptic curve summands of abelian varieties

Let $A/k$ be a principally polarized abelian variety of dimension $g$. In this section, we define the elliptic rank of $A$ to be the maximum number of elliptic curves appearing in a decomposition of $A$ up to isomorphism. When $A$ has $p$-rank 0, the elliptic rank is bounded by the superspecial rank, Proposition 4.2. Proposition 4.4 states that the elliptic rank is the number of rank 2 factors in the $p$-divisible group $A[p^\infty]$ when $A$ is supersingular.

### 4.1. Elliptic rank.

**Definition 4.1.** The *elliptic rank* $e(A)$ of $A$ is

$$e(A) := \max\{e \mid \iota : A \xrightarrow{\sim} A_1 \times (\times_{i=1}^{e} E_i)\}, \tag{4.1}$$

where $E_1, \dots, E_e$ are elliptic curves, $A_1$ is an abelian variety of dimension $g - e$, and $\iota$ is an isomorphism of abelian varieties over $k$.

(We remind the reader that many "cancellation problems" for abelian varieties have negative answers [33], and that the abelian variety $A_1$ in (4.1) is not necessarily unique.)

Here are some properties of the elliptic rank.

**Proposition 4.2.** *If $A$ has $p$-rank 0, then the elliptic rank is bounded by the superspecial rank: $e(A) \leq s(A)$.*

*Proof.* If $A$ has $p$-rank 0, then the elliptic curves $E_1, \dots, E_e$ in a maximal decomposition of $A$ are supersingular. Each supersingular curve in the decomposition contributes a factor of $\mathbb{E}/\mathbb{E}(F+V)$ to the Dieudonné module $\mathbb{D}_*(A[p])$. □

The proof of Proposition 3.12 shows that, for every $g \geq 2$ and prime $p$, there exists a supersingular principally polarized abelian variety of dimension $g$ over $k$ with elliptic rank $e$ if and only if $0 \leq e \leq g-2$ or $e = g$.

**Remark 4.3.** It is clear that $e(A) = 0$ if $A$ is simple and $\dim(A) > 1$. Recall from [15] that there exists a simple abelian variety $A$ with formal isogeny type $\eta$, for each non-supersingular Newton polygon $\eta$. It follows from Proposition 4.2 that there exist abelian varieties $A$ with $s(A) > 0$ and $e(A) = 0$ for all dimensions $g \geq 4$.

**4.2. Superspecial rank for *p*-divisible groups.** We briefly sketch a parallel version of superspecial rank in the category of $p$-divisible groups, rather than $p$-torsion group schemes. Many of the notions and results in Section 3.2 generalize to truncated Barsotti-Tate groups of arbitrary level, and indeed to Barsotti-Tate, or $p$-divisible, groups.

Let $\widetilde{G}$ be a pqp $p$-divisible group, and let $\widetilde{H} \subseteq \widetilde{G}$ be a sub-$p$-divisible group. We say that $\widetilde{H}$ is polarized if the principal quasipolarization on $\widetilde{G}$

restricts to one on $\widetilde{H}$. Lemma 3.4 admits an analogue for $p$-divisible groups; for such an $\widetilde{H}$, there exists a pqp complement $\widetilde{K}$ such that $\widetilde{G} \simeq \widetilde{H} \oplus \widetilde{K}$.

Let $\widetilde{I}_{1,1}$ be the $p$-divisible group whose Dieudonné module is

$$\widetilde{M}_{1,1} = \mathbb{D}_*(\widetilde{I}_{1,1}) \simeq \widetilde{\mathbb{E}}/\widetilde{\mathbb{E}}(F+V);$$

then $\widetilde{I}_{1,1}[p] \simeq I_{1,1}$.

With this preparation, we define the superspecial rank $\widetilde{s}(\widetilde{G})$ of a pqp $p$-divisible group $\widetilde{G}$ as the largest value of $s$ for which there exists a sub-pqp $p$-divisible group of $\widetilde{G}$ isomorphic to $\widetilde{I}_{1,1}^s$.

Since a decomposition of a $p$-divisible group induces a decomposition on its finite levels, it follows that

$$\widetilde{s}(\widetilde{G}) \leq s(\widetilde{G}[p]). \tag{4.2}$$

Similarly, if $A/k$ is a principally polarized abelian variety, then any decomposition of $A$ induces a decomposition of its $p$-divisible group. So if $A$ has $p$-rank 0, then

$$e(A) \leq \widetilde{s}(A[p^\infty]). \tag{4.3}$$

We thank Oort for suggesting the following result:

**Proposition 4.4.** *Let $A/k$ be a supersingular principally polarized abelian variety. Then*

$$e(A) = \widetilde{s}(A[p^\infty]).$$

*Proof.* Let $\widetilde{M}$ be the Dieudonné module $\widetilde{M} = \mathbb{D}_*(A[p^\infty])$, and let $E/k$ be a supersingular elliptic curve. Since $A$ is principally polarized, $\widetilde{M}$ is principally quasipolarized. Let $\widetilde{s} = \widetilde{s}(A[p^\infty])$. By the same proof as for Lemma 3.4, there is a decomposition of pqp Dieudonné modules

$$\widetilde{M} \simeq \widetilde{M}_{1,1}^{\widetilde{s}} \oplus \widetilde{N}, \tag{4.4}$$

where $\widetilde{N}$ has superspecial rank zero. By [23, Theorem 6.2], since $\widetilde{M}$ is supersingular, (4.4) induces a corresponding decomposition

$$A \simeq E^{\widetilde{s}} \oplus A_1. \tag{4.5}$$

where $A_1$ is a principally polarized abelian variety of dimension $g - \widetilde{s}$ with $\widetilde{s}(A_1[p^\infty]) = 0$. Thus $e(A) \geq \widetilde{s}$ and the result follows. □

**Remark 4.5.** In fact, it is not hard to give a direct proof that the existence of decomposition (4.4) implies the existence of (4.5). Indeed, since $A$ is supersingular, there exists an isogeny $\psi : E^g \to A$, which induces an isogeny of $p$-divisible groups $\psi[p^\infty] : \widetilde{I}_{1,1}^g \to A[p^\infty]$. Let $H = \mathrm{Ker}(\psi[p^\infty])$; it is a finite group scheme, and is thus also a sub-group scheme of $E^g$. Since $\mathrm{End}(\widetilde{I}_{1,1})$ is a maximal order in a division ring over $\mathbb{Z}_p$, it is a (noncommutative) principal ideal domain (see also [16, p. 335]). By the theory of

elementary divisors for such rings (e.g., [12, Chapter 3, Theorem 18]), there is an isomorphism $\widetilde{I}_{1,1}^g \simeq \widetilde{I}_{1,1}^{\widetilde{s}} \times \widetilde{I}_{1,1}^{g-\widetilde{s}}$ under which $H$ is contained in $0 \times \widetilde{I}_{1,1}^{g-\widetilde{s}}$. Since $\mathrm{End}(E^g[p^n]) \simeq \mathrm{End}(\widetilde{I}_{1,1}^g[p^n])$ for each $n \in \mathbb{N}$, there is an analogous decomposition $E^g \simeq E^{\widetilde{s}} \times E^{g-\widetilde{s}}$ under which $H$ is contained in $0 \times E^{g-\widetilde{s}}$. Then $A = E^g/N \simeq E^{\widetilde{s}} \oplus A_1$, where $A_1$ is supersingular but has superspecial rank zero.

**4.3. An open question.** Consider a principally polarized abelian variety $A/k$. By Remark 4.3, if $A$ is not supersingular, then it can be absolutely simple ($e(A) = 0$) and yet have positive superspecial rank ($s(A) > 0$). (Similarly, if $A$ admits ordinary elliptic curves as factors, then it is possible to have $e(A) > 0$ while $s(A) = 0$.)

However, if $A$ has $p$-rank 0, there are *a priori* inequalities

$$e(A) \leq \widetilde{s}(A[p^\infty]) \leq s(A[p]).$$

Proposition 4.4 shows the first inequality is actually an equality when $A$ is supersingular. This leads one to ask the following:

**Question 4.6.**

(1) If $A/k$ is supersingular, is $e(A) = s(A)$?
(2) If $\widetilde{G}$ is a supersingular pqp $p$-divisible group, is $\widetilde{s}(\widetilde{G}) = s(\widetilde{G}[p])$?

The two parts of Question 4.6 have the same answer by Proposition 4.4. Here is one difficulty in answering this question.

**Remark 4.7.** The $p$-divisible group $\widetilde{I}_{1,1}$ is isomorphic (over $k$) to the $p$-divisible group $H_{1,1}$ introduced in [13, 5.2]. Consequently, it is *minimal* in the sense of [28, page 1023]; if $\widetilde{M}$ is any Dieudonné module such that $(\widetilde{M} \otimes_W k) \simeq M_{1,1}^{\oplus s}$, then there is an isomorphism $\widetilde{M} \simeq \widetilde{M}_{1,1}^{\oplus s}$.

In spite of this, because of difficulties with extensions (see, e.g., [28, Remark 3.2]), one cannot immediately conclude that $\widetilde{M}$ admits $\widetilde{M}_{1,1}^{\oplus s}$ as a summand if $\widetilde{M}/p\widetilde{M}$ has superspecial rank $s$. Indeed, Lemma 3.9 indicates that an appeal to minimality alone is insufficient; any argument must make use of the principal quasipolarization.

## 5. Superspecial rank of supersingular Jacobians

If $X/k$ is a (smooth, projective, connected) curve, its superspecial and elliptic ranks are those of its Jacobian: $s(X) = s(\mathrm{Jac}(X))$ and $e(X) = e(\mathrm{Jac}(X))$. In this section, we address the question of which superspecial ranks occur for Jacobians of (supersingular) curves. First, recall that there is a severe restriction on the genus of a superspecial curve.

**Theorem 5.1** (Ekedahl)**.** *If $X/k$ is a superspecial curve of genus $g$, then $g \leq p(p-1)/2$* [5, Theorem 1.1]*, see also* [1].

For example, if $p = 2$, then the genus of a superspecial curve is at most 1. The Hermitian curve $X_p : y^p + y = x^{p+1}$ is a superspecial curve realizing the upper bound of Theorem 5.1.

In Section 5.2, we determine the superspecial ranks of all hyperelliptic curves in characteristic 2. We determine the superspecial rank of the Jacobians of Hermitian curves in Section 5.3. In both cases, this gives an upper bound for the elliptic rank.

**5.1. Supersingular Jacobians.** Recall that a curve $X/\mathbb{F}_q$ is *supersingular* if the Newton polygon of $L(X/\mathbb{F}_q, t)$ is a line segment of slope $1/2$ or, equivalently, if the Jacobian of $X$ is supersingular. One thing to note is that a curve $X/\mathbb{F}_q$ is supersingular if and only if $X$ is minimal over $\mathbb{F}_{q^c}$ for some $c \in \mathbb{N}$.

Van der Geer and Van der Vlugt proved that there exists a supersingular curve of every genus in characteristic $p = 2$ [9]. For $p \geq 3$, it is unknown if there exists a supersingular curve of every genus. An affirmative answer would follow from a conjecture about deformations of reducible supersingular curves [27, Conjecture 8.5.7]. There are many constructions of supersingular curves having arbitrarily large genus.

Recall (from proof of Proposition 3.12 and remarks after Proposition 4.2) that there exists a (non-simple) supersingular principally polarized abelian variety of dimension $g$ over $k$ with elliptic rank $e$ if and only if $0 \leq e \leq g-2$ or $e = g$. In light of this, one can ask the following question.

**Question 5.2.** Given $p$ prime and $g \geq 2$ and $0 \leq s \leq g-2$, does there exist a smooth curve $X$ over $\overline{\mathbb{F}}_p$ of genus $g$ whose Jacobian is supersingular and has elliptic rank $e$?

The answer to Question 5.2 is yes when $g = 2, 3$ and $e = 0$. To see this, recall from the proof of Lemma 3.11 that a generic supersingular principally polarized abelian variety of dimension $g$ has Dieudonné module $\mathbb{E}/\mathbb{E}(F^g + V^g)$, which has superspecial rank $s = 0$. When $g = 2, 3$, such an abelian variety is the Jacobian of a smooth curve with $e = 0$.

One expects the answer to Question 5.2 is yes when $g = 3$ and $e = 1$ also. To see this, let $E$ be a supersingular elliptic curve. Let $A$ be a supersingular, non-superspecial abelian surface. The 3-dimensional abelian variety $B = A \times E$ is supersingular and has superspecial rank 1. If there is a principal polarization on $B$ which is not the product polarization, then $B$ is the Jacobian of a smooth curve.

Question 5.2 is open for $g \geq 4$.

**5.2. Superspecial rank of hyperelliptic curves when $p = 2$.** In this section, suppose $k$ is an algebraically closed field of characteristic $p = 2$. Application 5.3 states that the superspecial rank of a hyperelliptic curve over $k$ with 2-rank 0 is either 0 or 1. More generally, Application 5.5 states

that the superspecial rank of a hyperelliptic curve over $k$ with 2-rank $r$ is bounded by $1 + r$.

A hyperelliptic curve $Y$ over $k$ is defined by an Artin-Schreier equation

$$y^2 + y = h(x),$$

for some non-constant rational function $h(x) \in k(x)$. In [6], the authors determine the structure of the Dieudonné module $M$ of $\mathrm{Jac}(Y)$ for all hyperelliptic curves $Y$ in characteristic 2. A surprising feature is that the isomorphism class of $M$ depends only on the orders of the poles of $h(x)$, and not on the location of the poles or otherwise on the coefficients of $h(x)$.

In particular, consider the case that the 2-rank of $Y$ is 0, or equivalently, that $h(x)$ has only one pole. In this case, the Ekedahl-Oort type is $[0, 1, 1, 2, 2, \ldots, \lfloor \frac{g}{2} \rfloor]$ [6, Corollary 5.3]. The $a$-number is $\lceil \frac{g}{2} \rceil$.

**Application 5.3.** Let $Y$ be a hyperelliptic curve of genus $g$ with 2-rank 0 defined over an algebraically closed field of characteristic 2. Then the superspecial rank of $\mathrm{Jac}(Y)$ is $s = 1$ if $g \equiv 1 \pmod 3$ and is $s = 0$ otherwise. The elliptic rank of $\mathrm{Jac}(Y)$ is $e \leq 1$ if $g \equiv 1 \pmod 3$ and $e = 0$ otherwise.

*Proof.* This follows by applying the algorithm in [6, Section 5.2]. Specifically, by [6, Proposition 5.10] (where $c = g$), the Dieudonné module of the group scheme with Ekedahl-Oort type $[0, 1, 1, 2, 2, \ldots, \lfloor \frac{g}{2} \rfloor]$ is generated by variables $X_j$ for $\lceil (g+1)/2 \rceil \leq j \leq g$ subject to the relations $F^{e(j)+1}(X_j) + V^{\epsilon(\iota(j))+1}(X_{\iota(j)})$, where the notation is defined in [6, Notation 5.9]. Then $M_{1,1}$ occurs as a summand if and only if there is some $j$ such that $e(j) = \epsilon(j) = 0$ and $j = \iota(j)$. The condition $e(j) = 0$ is equivalent to $j$ being odd. The conditions $\epsilon(j) = 0$ and $j = \iota(j)$ imply that $2g - 2j + 1 = g - (j-1)/2$ which is possible only if $g \equiv 1 \bmod 3$. If $g \equiv 1 \bmod 3$, then $j = (2g+1)/3$ so the maximal rank of a summand isomorphic to $I_{1,1}^s$ is $s = 1$. □

**Remark 5.4.** It is not known exactly which natural numbers $g$ can occur as the genus of a supersingular hyperelliptic curve over $\overline{\mathbb{F}}_2$. On one hand, if $g = 2^s - 1$, then there does not exist a supersingular hyperelliptic curve of genus $g$ over $\overline{\mathbb{F}}_2$ [31].

On the other hand, if $h(x) = xR(x)$ for an additive polynomial $R(x)$ of degree $2^s$, then $Y$ is supersingular of genus $2^{s-1}$ [8]. If $s$ is even, then Application 5.3 shows that $\mathrm{Jac}(Y)$ has no elliptic curve factors in a decomposition up to isomorphism, even though it decomposes completely into elliptic curves up to isogeny.

More generally, we now determine the superspecial ranks of hyperelliptic curves in characteristic 2 having arbitrary 2-rank. Consider the divisor of

poles

$$\mathrm{div}_\infty(h(x)) = \sum_{j=0}^{r} d_j P_j.$$

By Artin-Schreier theory, one can suppose that $d_j$ is odd for all $j$. Then $\mathrm{Jac}(Y)$ has genus $g$ satisfying $2g+2 = \sum_{j=0}^{r}(d_j+1)$ by the Riemann-Hurwitz formula [32, IV, Prop. 4] and has 2-rank $f = r$ by the Deuring-Shafarevich formula [34, Theorem 4.2] or [2, Cor. 1.8]. These formulae imply that, for a given genus $g$ (and 2-rank $r$), there is another discrete invariant of a hyperelliptic curve $Y/k$, namely a partition of $2g+2$ into $r+1$ positive even integers $d_j+1$. In [6], the authors prove that the Ekedahl-Oort type of $Y$ depends only on this discrete invariant.

Specifically, consider the variable $x_j := (x-P_j)^{-1}$, which is the inverse of a uniformizer at the branch point $P_j$ in $\mathbb{P}^1$ (with $x_j = x$ if $P_j = \infty$). Then $h(x)$ has a partial fraction decomposition of the form

$$h(x) = \sum_{j=0}^{r} h_j(x_j),$$

where $h_j(x) \in k[x]$ is a polynomial of degree $d_j$. Let $c_j = (d_j-1)/2$ and note that $g = r + \sum_{j=0}^{r} c_j$. For $0 \le j \le r$, consider the Artin-Schreier $k$-curve $Y_j$ with affine equation $y^2 - y = h_j(x)$. Let $E_0$ be an ordinary elliptic curve over $k$.

Then [6, Theorem 1.2] states that the de Rham cohomology of $Y$ decomposes, as a module under the actions of Frobenius $F$ and Verschiebung $V$, as:

$$H^1_{\mathrm{dR}}(Y) \simeq H^1_{\mathrm{dR}}(E_0)^r \oplus \bigoplus_{j=0}^{r} H^1_{\mathrm{dR}}(Y_j).$$

Since $E_0$ is ordinary, it has superspecial rank 0. The superspecial rank of $\mathrm{Jac}(Y)$ is thus the sum of the superspecial ranks of $\mathrm{Jac}(Y_j)$. Applying Application 5.3 to $\{Y_j\}_{j=0}^{r}$ proves the following.

**Application 5.5.** Consider a hyperelliptic curve $Y$ defined over an algebraically closed field of characteristic 2. Then $Y$ is defined by an equation of the form $y^2+y = h(x)$ with $\mathrm{div}_\infty(h(x)) = \sum_{j=0}^{r} d_j P_j$ and $d_j$ odd. Recall that $Y$ has genus $g = r + \sum_{j=0}^{r} c_j$ where $c_j = (d_j-1)/2$ and $p$-rank $r$. The superspecial rank of $\mathrm{Jac}(Y)$ equals the number of $j$ such that $c_j \equiv 1 \bmod 3$. In particular, $s(\mathrm{Jac}(Y)) \le 1+r$ and $e((\mathrm{Jac}(Y))) \le 1+2r$.

**5.3. Hermitian curves.** The last examples of the paper are about the superspecial rank for one of the three classes of (supersingular) Deligne-Lusztig curves: the Hermitian curves $X_q$ for $q = p^n$ for an arbitrary prime $p$. In most cases, the superspecial (and elliptic) ranks are quite small, which

is somewhat surprising since these curves are exceptional from many perspectives.

Let $q = p^n$. The Hermitian curve $X_q$ has affine equation

$$y^q + y = x^{q+1}.$$

It is supersingular with genus $g = q(q-1)/2$. It is maximal over $\mathbb{F}_{q^2}$ because $\#X_q\left(\mathbb{F}_{q^2}\right) = q^3 + 1$. The zeta function of $X_q$ is

$$Z(X_q/\mathbb{F}_q, t) = \frac{(1+qt^2)^g}{(1-t)(1-qt)}.$$

In fact, $X_q$ is the unique curve of this genus which is maximal over $\mathbb{F}_{q^2}$ [30]. This was used to prove that $X_q$ is the Deligne-Lusztig variety for $\mathrm{Aut}(X_q) = \mathrm{PGU}(3, q)$ [11, Proposition 3.2].

By [10, Proposition 14.10], the $a$-number of $X_q$ is

$$a = p^n(p^{n-1} + 1)(p-1)/4,$$

which equals $g$ when $n = 1$, equals $g/2$ when $n = 2$, and is approximately $g/2$ for $n \geq 3$. In particular, $X_{p^n}$ is superspecial if and only if $n = 1$.

In [29], for all $q = p^n$, the authors determine the Dieudonné module $\mathbb{D}_*(X_q) = \mathbb{D}_*(\mathrm{Jac}(X_q)[p])$, complementing earlier work in [3, 4]. In particular, [29, Theorem 5.13] states that the distinct indecomposable factors of Dieudonné module $\mathbb{D}_*(X_q)$ are in bijection with orbits of $\mathbb{Z}/(2^n+1) - \{0\}$ under $\times 2$. Each factor's structure is determined by the combinatorics of the orbit, which depends only on $n$ and not on $p$. The multiplicities of the factors do depend on $p$. For example, when $n = 2$, the Dieudonné module of $X_{p^2}$ is $M_{2,2}^{g/2}$, which has superspecial rank 0 (Lemma 3.9). Here is an application of these results.

**Application 5.6.** The elliptic rank of the Jacobian of the Hermitian curve $X_{p^n}$ equals 0 if $n$ is even and is at most $(\frac{p(p-1)}{2})^n$ if $n$ is odd.

*Proof.* By Proposition 4.2, $e(\mathrm{Jac}(X_{p^n})) \leq s(\mathrm{Jac}(X_{p^n}))$. Applying [29, Application 6.1], the factor $\mathbb{E}/\mathbb{E}(F+V)$ occurs in the Dieudonné module if and only if there is an orbit of length 2 in $\mathbb{Z}/(2^n+1)$ under $\times 2$. This happens if and only if there is an element of order three in $\mathbb{Z}/(2^n+1)$, which is true if and only if $n$ is odd. If $n$ is odd, this shows that $\mathbb{E}/\mathbb{E}(F+V)$ is not a factor of the Dieudonné module and $s(\mathrm{Jac}(X_{p^n})) = 0$. If $n$ is even, the multiplicity of this factor is $s(\mathrm{Jac}(X_{p^n})) = (\frac{p(p-1)}{2})^n$. □

## References

[1] M. H. Baker, "Cartier points on curves", *Internat. Math. Res. Notices* (2000), no. 7, p. 353-370.

[2] R. M. Crew, "Etale $p$-covers in characteristic $p$", *Compositio Math.* **52** (1984), no. 1, p. 31-45.

[3] N. Dummigan, "The determinants of certain Mordell-Weil lattices", *Amer. J. Math.* **117** (1995), no. 6, p. 1409-1429.
[4] ———, "Complete $p$-descent for Jacobians of Hermitian curves", *Compositio Math.* **119** (1999), no. 2, p. 111-132.
[5] T. Ekedahl, "On supersingular curves and abelian varieties", *Math. Scand.* **60** (1987), no. 2, p. 151-178.
[6] A. Elkin & R. Pries, "Ekedahl-Oort strata of hyperelliptic curves in characteristic 2", *Algebra Number Theory* **7** (2013), no. 3, p. 507-532.
[7] H. Friedlander, D. Garton, B. Malmskog, R. Pries & C. Weir, "The $a$-numbers of Jacobians of Suzuki curves", *Proc. Amer. Math. Soc.* **141** (2013), no. 9, p. 3019-3028.
[8] G. van der Geer & M. van der Vlugt, "Reed-Muller codes and supersingular curves. I", *Compositio Math.* **84** (1992), no. 3, p. 333-367.
[9] ———, "On the existence of supersingular curves of given genus", *J. Reine Angew. Math.* **458** (1995), p. 53-61.
[10] B. H. Gross, "Group representations and lattices", *J. Amer. Math. Soc.* **3** (1990), no. 4, p. 929-960.
[11] J. P. Hansen, "Deligne-Lusztig varieties and group codes", in *Coding theory and algebraic geometry (Luminy, 1991)*, Lecture Notes in Math., vol. 1518, Springer, Berlin, 1992, p. 63-81.
[12] N. Jacobson, *The Theory of Rings*, American Mathematical Society Mathematical Surveys, vol. II, American Mathematical Society, New York, 1943, vi+150 pages.
[13] A. J. de Jong & F. Oort, "Purity of the stratification by Newton polygons", *J. Amer. Math. Soc.* **13** (2000), no. 1, p. 209-241.
[14] H. Kraft, "Kommutative algebraische p-Gruppen (mit Anwendungen auf p-divisible Gruppen und abelsche Varietäten)", manuscript, University of Bonn, September 1975, 86 pp.
[15] H. W. Lenstra, Jr. & F. Oort, "Simple abelian varieties having a prescribed formal isogeny type", *J. Pure Appl. Algebra* **4** (1974), p. 47-53.
[16] K. Z. Li, "Classification of supersingular abelian varieties", *Math. Ann.* **283** (1989), no. 2, p. 333-351.
[17] K.-Z. Li & F. Oort, *Moduli of supersingular abelian varieties*, Lecture Notes in Mathematics, vol. 1680, Springer-Verlag, Berlin, 1998, iv+116 pages.
[18] J. I. Manin, "Theory of commutative formal groups over fields of finite characteristic", *Uspehi Mat. Nauk* **18** (1963), no. 6 (114), p. 3-90.
[19] B. Moonen, "Group schemes with additional structures and Weyl group cosets", in *Moduli of abelian varieties (Texel Island, 1999)*, Progr. Math., vol. 195, Birkhäuser, Basel, 2001, p. 255-298.
[20] N. O. Nygaard, "Slopes of powers of Frobenius on crystalline cohomology", *Ann. Sci. École Norm. Sup. (4)* **14** (1981), no. 4, p. 369-401 (1982).
[21] T. Oda, "The first de Rham cohomology group and Dieudonné modules", *Ann. Sci. École Norm. Sup. (4)* **2** (1969), p. 63-135.
[22] T. Oda & F. Oort, "Supersingular abelian varieties", in *Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977)*, Kinokuniya Book Store, Tokyo, 1978, p. 595-621.
[23] A. Ogus, "Supersingular $K3$ crystals", in *Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. II*, Astérisque, vol. 64, Soc. Math. France, Paris, 1979, p. 3-86.
[24] F. Oort, "Subvarieties of moduli spaces", *Invent. Math.* **24** (1974), p. 95-119.
[25] ———, "Which abelian surfaces are products of elliptic curves?", *Math. Ann.* **214** (1975), p. 35-47.
[26] ———, "A stratification of a moduli space of abelian varieties", in *Moduli of abelian varieties (Texel Island, 1999)*, Progr. Math., vol. 195, Birkhäuser, Basel, 2001, p. 345-416.
[27] ———, "Abelian varieties isogenous to a Jacobian", *Rend. Sem. Mat. Univ. Padova* **113** (2005), p. 165-172.
[28] ———, "Minimal $p$-divisible groups", *Ann. of Math. (2)* **161** (2005), no. 2, p. 1021-1036.
[29] R. Pries & C. Weir, "Ekedahl-Oort type of Jacobians of Hermitian curves", to appear in *Asian J. Math.*, `http://arxiv.org/abs/1302.6261`.

[30] H.-G. Rück & H. Stichtenoth, "A characterization of Hermitian function fields over finite fields", *J. Reine Angew. Math.* **457** (1994), p. 185-188.
[31] J. Scholten & H. J. Zhu, "Hyperelliptic curves in characteristic 2", *Int. Math. Res. Not.* (2002), no. 17, p. 905-917.
[32] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII, 245 pages.
[33] T. Shioda, "Some remarks on Abelian varieties", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **24** (1977), no. 1, p. 11-21.
[34] D. Subrao, "The $p$-rank of Artin-Schreier curves", *Manuscripta Math.* **16** (1975), no. 2, p. 169-193.
[35] J. Tate, "Endomorphisms of abelian varieties over finite fields", *Invent. Math.* **2** (1966), p. 134-144.
[36] D. L. Ulmer, "$p$-descent in characteristic $p$", *Duke Math. J.* **62** (1991), no. 2, p. 237-265.

Jeffrey D. Achter
Colorado State University
Fort Collins, CO, 80521
USA
*E-mail*: achter@math.colostate.edu
*URL*: http://www.math.colostate.edu/~achter/

Rachel Pries
Colorado State University
Fort Collins, CO, 80521
USA
*E-mail*: pries@math.colostate.edu
*URL*: http://www.math.colostate.edu/~pries/