Superspecial rank of supersingular curves

Rachel Pries

Colorado State University
pries@math.colostate.edu

November 13

RICAM Algebraic Curves over Finite Fields
Abstract: A curve $X$ of genus $g$ over a finite field is *supersingular* if the Newton polygon of its $L$-polynomial is a line segment of slope $1/2$.

Equivalently, $X$ is supersingular if and only if the Jacobian $\text{Jac}(X)$ is isogenous to a product of supersingular elliptic curves.

Only in rare cases is $\text{Jac}(X)$ isomorphic to a product of supersingular elliptic curves, in which case $X$ is called *superspecial*.

I will define the *superspecial rank*, which is an invariant of the Dieudonné module or Ekedahl-Oort type of a p.p. abelian variety.

If $X$ is a supersingular curve, then the superspecial rank determines the number of elliptic factors in the decomposition of $\text{Jac}(X)$ up to isomorphism.

As examples, we compute the superspecial rank of Hermitian curves and Suzuki curves. I will describe results about the superspecial rank of curves in characteristic 2.
Overview

An elliptic curve $E/F_p$ can be ordinary or supersingular. How do you generalize supersingular property? Study: abelian varieties of dimension $g > 1$ and curves of genus $g > 1$.

A. $p$-rank $f = 0$
B. supersingular
C. superspecial

Today: define superspecial rank (invariant of Dieudonné module) differentiating B and C for curves

Motivation - supersingular elliptic rank of supersingular Jacobians
Examples (with Elkin, Weir, Malmskog)

Another day: Newton polygon results - differentiating A and B for curves
Let $E$ be a smooth elliptic curve over $k = \overline{k}$, with $\text{char}(k) = p$. Let $E[p]$ be the kernel of the inseparable multiplication-by-$p$ morphism.

$E$ is **supersingular** if it satisfies the following equivalent conditions:

A. The only $p$-torsion point is the identity: $E[p](k) = \{ \text{id} \}$.

B. The Newton polygon of $E$ is a line segment of slope $\frac{1}{2}$.

C. The group scheme $E[p]$ contains 1 copy of $\alpha_p$, the kernel of Frobenius on $\mathbb{G}_a$.

For all $p$, there exists a supersingular elliptic curve $E$ over $\mathbb{F}_{p^2}$ (Igusa).
Let $A$ be a p.p. abelian variety of dimension $g$ over $k = \bar{k}$, char($k$) = $p$. Let $A[p]$ be the kernel of the inseparable multiplication-by-$p$ morphism.

The following conditions are all different for $g \geq 3$.

**A. $p$-rank 0** - The only $p$-torsion point is the identity: $A[p](k) = \{\text{id}\}$.

**B. supersingular** - The Newton polygon of $A$ is a line of slope $\frac{1}{2}$.

**C. superspecial** - The group scheme $A[p]$ contains $g$ copies of $\alpha_p$, the kernel of Frobenius on $\mathbb{G}_a$.

Then $C \Rightarrow B \Rightarrow A$.

**Goal:** study $A \not\Rightarrow B \not\Rightarrow C$ for Jacobians of curves of genus $g \geq 3$. 
B. Definition of Newton polygon

Let $X$ be a smooth projective curve defined over $\mathbb{F}_q$. Zeta function of $X$ is $Z(X/\mathbb{F}_q, t) = L(X/\mathbb{F}_q, t)/(1 - t)(1 - qt)$

where $L(X/\mathbb{F}_q, t) = \prod_{i=1}^{2g} (1 - w_i t) \in \mathbb{Z}[t]$ and $|w_i| = \sqrt{q}$.

The Newton polygon of $X$ is the NP of the $L$-polynomial $L(t)$. Find $p$-adic valuation $v_i$ of coefficient of $t^i$ in $L(t)$. Draw lower convex hull of $(i, v_i/a)$ where $q = p^a$.

**Facts:** The NP goes from $(0, 0)$ to $(2g, g)$. NP line segments break at points with integer coefficients; If slope $\lambda$ occurs with length $m_\lambda$, so does slope $1 - \lambda$.

**Definition**

$X/\mathbb{F}_q$ is *supersingular* if the Newton polygon of $L(X/\mathbb{F}_q, t)$ is a line segment of slope $1/2$.

There is a partial ordering on NPs; the supersingular NP is ’smallest’. 
Let $A$ be a p.p. abelian variety of dimension $g$ over $k$.

**Manin:** for $c, d$ relatively prime s.t. $\lambda = \frac{c}{d} \in \mathbb{Q} \cap [0, 1]$, define a $p$-divisible group $G_{c,d}$ of dimension $c$ and height $d$.

The Dieudonné module $D_\lambda$ for $G_{c,d}$ is a $W(k)$-module. Over $\text{Frac}(W(k))$, there is a basis $x_1, \ldots, x_d$ for $D_\lambda$ s.t. $F^d x_i = p^c x_i$.

There is an isogeny of $p$-divisible groups $A[p^\infty] \sim \bigoplus_\lambda G_{c,d}^{m_\lambda}$.

Newton polygon:
lower convex hull - line segments of slope $\lambda$ and length $m_\lambda$.

**Definition:** A supersingular iff $\lambda = \frac{1}{2}$ is the only slope.
Existence of supersingular objects

**Abelian varieties:**
For all $p$ and $g$, there exists a supersingular p.p. abelian variety of dimension $g$, namely $E^g$.

Let $\mathcal{A}_g$ be the moduli space of p.p. abelian varieties of dimension $g$. The supersingular locus of $\mathcal{A}_g$ has dimension $\left\lfloor \frac{g^2}{4} \right\rfloor$.

**Smooth Curves:** Many experts on supersingular curves are here.

**Van der Geer/Van der Vlugt:**
If $p = 2$, there exists a supersingular curve of every genus.

**Open problem**
For $p \geq 3$, it is unknown if there exists a supersingular curve of every genus.
Let \( q = p^n \). The *Hermitian curve* \( X_q \) has affine equation \( y^q + y = x^{q+1} \).

It has genus \( g = q(q - 1)/2 \).
It is maximal over \( \mathbb{F}_{q^2} \) because \( \#X_q(\mathbb{F}_{q^2}) = q^3 + 1 \).

**Ruck/Stichtenoth:** \( X_q \) is unique curve of genus \( g \) maximal over \( \mathbb{F}_{q^2} \).

**Hansen:** \( X_q \) is the Deligne-Lusztig variety for \( \text{Aut}(X_q) = \text{PGU}(3, q) \).

The zeta function of \( X_q \) is \( Z(X_q/\mathbb{F}_q, t) = \frac{(1+qt^2)^g}{(1-t)(1-qt)} \).
The only slope of the Newton polygon of \( L(t) = (1 + qt^2)^g \) is \( 1/2 \).

Thus \( \text{Jac}(X_q) \) is supersingular.
C. The group scheme $E[p]$ contains 1 copy of $\alpha_p$, the kernel of Frobenius on $\mathbb{G}_a$.

As a $k$-scheme, $\alpha_p \simeq \text{Spec}(k[x]/x^p)$ with co-multiplication $m^*(x) = x \otimes 1 + 1 \otimes x$ and co-inverse $\text{inv}^*(x) = -x$.

$E[p]$ is a group scheme of rank $p^2$, fitting in a non-split exact sequence

$$0 \to \alpha_p \to E[p] \to \alpha_p \to 0.$$ 

The image of $\alpha_p$ is the kernel of $F$ (Frobenius) and $V$ (Verschiebung).

What is a good generalization of this condition?
First approach - the a-number

Let $\alpha_p$ denote the kernel of Frobenius on $G_a$.

**Definition**

The $a$-number of $A$ is $a(A) = \dim_k \text{Hom}(\alpha_p, A[p])$.

**Computation:** Let $X$ be a curve of genus $g$. Let $r$ be the rank of the Cartier operator on $H^0(X, \Omega^1)$. Then the $a$-number of $A = \text{Jac}(X)$ is $a = g - r$.

**Example - the Hermitian curve**

Let $q = p^n$. Recall that $X_q : y^q + y = x^{q+1}$ has genus $g = q(q-1)/2$.

If $n = 1$, then $a = g$. If $n = 2$, then $a = g/2$.

Gross: $a = p^n(p^{n-1} + 1)(p - 1)/4$. 
Computation of $a$-number of Hermitian curve

The Cartier operator $C$ acts on $H^0(X_q, \Omega^1)$.

Let $\Delta = \{(i,j) \mid i,j \in \mathbb{Z}, \ i,j \geq 0, \ i+j \leq q-2\}$. A basis for $H^0(X_q, \Omega^1)$ is $B = \{\omega_{i,j} := x^i y^j dx \mid (i,j) \in \Delta\}$.

Write $i = i_0 + pi_T^n$ and $j = j_0 + pj_T^n$ with $0 \leq i_0, j_0 \leq p - 1$.

\[
C(x^i y^j dx) = x^{i_T^n} y^{j_T^n} C(x^{i_0} (x^{q+1} - y^q)^{j_0} dx)
\]
\[
= x^{i_T^n} y^{j_T^n} \sum_{l=0}^{j_0} \binom{j_0}{l} (-1)^l x^{p^{n-1} (j_0 - l)} y^{p^{n-1} l} C(x^{i_0 + j_0 - l} dx).
\]

$C(x^k dx) \neq 0$ iff $k \equiv -1 \mod p$. Need $i_0 + j_0 - \ell \equiv -1 \mod p$.

If $i_0 + j_0 < p - 1$, then $C(\omega_{i,j}) = 0$.
If $i_0 + j_0 \geq p - 1$, then $C(\omega_{i,j}) = \omega^{p^{n-1} (p-1-i_0) + i_T^n, p^{n-1} (i_0+j_0-(p-1)) + j_T^n}$. 

Pries (CSU)

special rank of singular curves

November 13

12 / 36
C. Superspecial

Let $A$ be a p.p. abelian variety of dimension $g$ over $k = \bar{k}$, $\text{char}(k) = p$.

Recall $a(A) = \dim_k \text{Hom}(\alpha_p, A[p])$, with $\alpha_p$ kernel of Frobenius on $\mathbb{G}_a$.

**Def:** An abelian variety $A$ is *superspecial* if $a(A) = g$.

Let $E$ be a supersingular elliptic curve over $k$.

Oort

$A$ is supersingular iff $A \sim E^g$ is ISOGENOUS to a product of supersingular elliptic curves.

$A$ is superspecial iff $A \simeq \times_{i=1}^g E_i$ is ISOMORPHIC to a product of supersingular elliptic curves.
Existence of superspecial objects

**Abelian varieties:** The number of superspecial p.p. abelian varieties of dim $g$ is finite and non-zero; (it is a class number).

The superspecial locus of $A_g$ has dimension 0.

**Smooth curves:** Problem: there are not many superspecial curves.

**Example:** The Hermitian curve $X_q : y^q + y = x^{q+1}$ is supersingular for all $q = p^n$, but superspecial iff $n = 1$.

**Ekedahl**

If $X/\overline{F}_p$ is a superspecial curve of genus $g$, then $g \leq p(p - 1)/2$.

Upper bound realized by Hermitian curve $X_p : y^p + y = x^{p+1}$. 
Another approach - Dieudonné module


Here $E = k[F, V]$ is the non-commutative ring generated by semi-linear operators $F$ and $V$ with relations $FV = VF = 0$ and $F\lambda = \lambda^p F$ and $\lambda V = V\lambda^p$ for all $\lambda \in k$.

Let $(R) = ER$ be the left ideal of $E$ generated by $R$.

Let $E$ be a supersingular elliptic curve.
Let $I_{1,1}$ be the isomorphism class of the rank $p^2$ group scheme $E[p]$.
The Dieudonné module of $I_{1,1}$ is $E/(F + V)$

Fact:

$A$ is superspecial if and only if $A[p] \simeq (I_{1,1})^g$.
$A$ is superspecial if and only if $D(A[p]) = (E/(F + V))^g$.
Let \( q = p^n \). Recall that \( X_q : y^q + y = x^{q+1} \) has genus \( g = q(q - 1)/2 \). Let \( \mathcal{D}(X_q) \) denote the Dieudonné module of \( \text{Jac}(X_q)[p] \).

**Theorem - Pries/Weir**

We determine the Dieudonné module \( D(X_q) \) for all \( q = p^n \), complementing earlier work of Dummigan. Its distinct indecomposable factors are in bijection with orbits of \( \mathbb{Z}/(2^n + 1) - \{0\} \) under \( \times 2 \).

**Examples:**

\[
\begin{align*}
\mathcal{D}(X_p) &= \left( \mathbb{E}/(F + V) \right)^g. \\
\mathcal{D}(X_{p^2}) &= \left( \mathbb{E}/(F^2 + V^2) \right)^{g/2}.
\end{align*}
\]

\[
\mathcal{D}(X_{p^3}) = \left( \mathbb{E}/\mathbb{E}(F^3 + V^3) \right)^{r_{3,2}} \oplus \left( \mathbb{E}/\mathbb{E}(F + V) \right)^{g - 3r_{3,2}},
\]

where \( r_{3,2} = p^3(p+1)^2(p-1)/2^3 \).
Let \( X \) be a supersingular curve of genus \( g \).

Recall that \( \text{Jac}(X) \sim E^g \) with \( E \) supersingular elliptic curve.

But, almost always, \( \text{Jac}(X) \not\cong \times_{i=1}^{g} E_i \).

Find an invariant that measures the extent to which \( \text{Jac}(X) \) decomposes up to isomorphism.

The \( a \)-number is not good. Could have large \( a \)-number even when \( \text{Jac}(X) \) indecomposable.

The Dieudonné module is too complicated. There are \( 2^g \) options for the DM, \( 2^{g-1} \) when the \( p \)-rank is \( f = 0 \). The DM could have many factors even when \( \text{Jac}(X) \) indecomposable.
Superspecial rank

Let $A$ be a p.p. abelian variety of dimension $g$ over $k$.

**Definition**

The *superspecial rank* $s(A)$ is the multiplicity of $\mathbb{E}/(F + V)$ in the Dieudonné module of $A[p]$.

**Fact**: $s(A)$ is the dimension of $\ker(F + V)$ on $H^1_{\text{dR}}(A)$.

If $A$ ordinary, then $s(A) = 0$.

In fact, $0 \leq s(A) \leq a(A) \leq g - f(A)$

because each factor of $\mathbb{E}/(F + V)$ contributes to the $a$-number and
because $f(A)$ is the multiplicity of $\mathbb{Z}/p \oplus \mu_p$ in $A[p]$.

Also $s(A) = g$ iff $A$ is superspecial.
The isomorphism type of the $p$-torsion of an elliptic curve $E$ is:
$L = \mathbb{Z}/p \oplus \mu_p$ if $E$ is ordinary
$I_{1,1}$ if $E$ is supersingular

Here $\mathbb{E}$ is the non-commutative ring generated by semi-linear operators $F$ and $V$ with the relations $FV = VF = 0$ and $F\lambda = \lambda^p F$ and $\lambda V = V\lambda^p$ for all $\lambda \in k$; and $(\rho)$ denotes the left ideal of $\mathbb{E}$ generated by $\rho$. 

<table>
<thead>
<tr>
<th>Name</th>
<th>cod</th>
<th>$f$</th>
<th>$a$</th>
<th>$v$</th>
<th>$\mu$</th>
<th>Dieudonné module</th>
<th>$s(A)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>[1]</td>
<td>0</td>
<td>$\mathbb{E}/(F, 1 - V) \oplus \mathbb{E}/(V, 1 - F)$</td>
<td>0</td>
</tr>
<tr>
<td>$I_{1,1}$</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>[0]</td>
<td>{1}</td>
<td>$\mathbb{E}/(F + V)$</td>
<td>1</td>
</tr>
</tbody>
</table>
Example - dimension $g = 2$:

<table>
<thead>
<tr>
<th>Name</th>
<th>cod</th>
<th>$f$</th>
<th>$a$</th>
<th>$\nu$</th>
<th>$\mu$</th>
<th>Dieudonné module</th>
<th>$s(A)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L^2$</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>[1, 2]</td>
<td>$0$</td>
<td>$D(L)^2$</td>
<td>0</td>
</tr>
<tr>
<td>$L \oplus l_{1,1}$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>[1, 1]</td>
<td>${1}$</td>
<td>$D(L) \oplus \mathbb{E}/(F + V))$</td>
<td>1</td>
</tr>
<tr>
<td>$l_{2,1}$</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>[0, 1]</td>
<td>${2}$</td>
<td>$\mathbb{E}/(F^2 + V^2)$</td>
<td>0</td>
</tr>
<tr>
<td>$l_{1,1}^2$</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>[0, 0]</td>
<td>${2, 1}$</td>
<td>$(\mathbb{E}/(F + V))^2$</td>
<td>2</td>
</tr>
</tbody>
</table>

The supersingular locus contains both types $(l_{1,1})^2$ and $l_{2,1}$.
### Dimension $g = 3$:

<table>
<thead>
<tr>
<th>Name</th>
<th>cod</th>
<th>$f$</th>
<th>$a$</th>
<th>$\nu$</th>
<th>Dieudonné module</th>
<th>$s(A)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L^3$</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>$[1,2,3]$</td>
<td>$D(L)^3$</td>
<td>0</td>
</tr>
<tr>
<td>$L^2 \oplus I_{1,1}$</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>$[1,2,2]$</td>
<td>$D(L)^2 \oplus \mathbb{E}/(F + V)$</td>
<td>1</td>
</tr>
<tr>
<td>$L \oplus I_{2,1}$</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>$[1,1,2]$</td>
<td>$D(L) \oplus \mathbb{E}/(F^2 + V^2)$</td>
<td>0</td>
</tr>
<tr>
<td>$L \oplus I^2_{1,1}$</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>$[1,1,1]$</td>
<td>$D(L) \oplus (\mathbb{E}/(F + V))^2$</td>
<td>2</td>
</tr>
<tr>
<td>$I_{3,1}$</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>$[0,1,2]$</td>
<td>$\mathbb{E}/(F^3 + V^3)$</td>
<td>0</td>
</tr>
<tr>
<td>$I_{3,2}$</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>$[0,1,1]$</td>
<td>$\mathbb{E}/(F^2 - V) \oplus \mathbb{E}/(V^2 - F)$</td>
<td>0</td>
</tr>
<tr>
<td>$I_{1,1} \oplus I_{2,1}$</td>
<td>5</td>
<td>0</td>
<td>2</td>
<td>$[0,0,1]$</td>
<td>$\mathbb{E}/(F + V) \oplus \mathbb{E}/(F^2 + V^2)$</td>
<td>1</td>
</tr>
<tr>
<td>$I^3_{1,1}$</td>
<td>6</td>
<td>0</td>
<td>3</td>
<td>$[0,0,0]$</td>
<td>$(\mathbb{E}/(F + V))^3$</td>
<td>3</td>
</tr>
</tbody>
</table>

The group scheme $A[p]$ does not determine the NP of $A$ when $g \geq 3$.

If $A[p] \simeq I_{3,1}$, then the NP of $A$ is usually $G_{1,2} + G_{2,1}$ (three slopes of $1/3$ and $2/3$) but it can also be $3G_{1,1}$ (supersingular).
The \( p \)-torsion \( A[p] \) is a group scheme of rank \( p^{2g} \).

The isomorphism class of \( A[p] \) is determined by its Ekedahl-Oort type.

Find final filtration \( N_1 \subset \cdots \subset N_{2g} \) of \( D(A[p]) \) as \( k \)-vector space, stable under the action of \( V \) and \( F^{-1} \) such that \( i = \dim(N_i) \).

The \textit{Ekedahl-Oort type} is \( \nu = [\nu_1, \ldots, \nu_g] \) where \( \nu_i = \dim(V(N_i)) \).

There are nec/suff conditions \( \nu_i \leq \nu_{i+1} \leq \nu_i + 1 \) on \( \nu \).

There are \( 2^g \) possibilities for the isomorphism class of \( A[p] \).
Lemma

For all $p$ and $g \geq 2$, a generic supersingular p.p. abelian variety has superspecial rank 0.

Proof: A generic supersingular p.p. abelian variety has $p$-rank 0 and $a$-number 1 Li/Oort.

This forces DM to be $\mathbb{E}/(F^g + V^g)$, thus superspecial rank 0 for $g \geq 2$.

Remark:
Most abelian varieties with $DM = \mathbb{E}/(F^g + V^g)$ are not supersingular. An EO strata is fully contained in supersingular locus iff smaller than $[0, 0, \ldots, 0, 1, 2, \ldots, \lfloor \frac{g}{2} \rfloor]$.
Supersingular ranks of supersingular abelian varieties

Classify all the supersingular ranks which occur for supersingular abelian varieties

**Proposition**

For all \( p \) and \( g \), there exists a supersingular abelian variety of dimension \( g \) over \( \overline{\mathbb{F}}_p \) with superspecial rank \( s \) if and only if \( 0 \leq s \leq g - 2 \) or \( s = g \).

**Proof sketch:**

There exists a supersingular abelian variety \( A_1 \) of dim \( g - s \) with \( a = 1 \).

The DM is \( E/(F^{g-s} + V^{g-s}) \) so \( s(A_1) = 0 \) as long as \( s \neq g - 1 \).

Let \( A = E^s \times A_1 \) where \( E \) is a supersingular elliptic curve.
Let $K$ be the function field of a curve over $k$ and $v$ place of $K$.
Let $f : A \to A'$ be an isogeny of abelian varieties over $K$.

**Motivation - superspecial rank**

Let $A$ be a constant supersingular elliptic curve over $K$ and $f = [p]$. Ulmer: The rank of $\text{Sel}(K, [p])$ is the superspecial rank.

Tate-Shafarevich group: $\Sha(K, A)_f = \ker(\Sha(K, A) \to \Sha(K, A'))$
where $\Sha(K, A) = \ker(H^1(K, A) \to \prod_v H^1(K_v, A))$.

Selmer group: $\text{Sel}(K, f)$ is subset of $H^1(K, \ker(f))$ s.t. restriction is in image of $\text{Sel}(K_v, f) = \text{Im}(A'(K_v) \to H^1(K_v, \ker(f)))$ for all $v$.

Exact sequence $0 \to A'(K)/f(A(K)) \to \text{Sel}(K, f) \to \Sha(K, A)_f \to 0$. 
Let $A$ be an abelian variety of dimension $g$ over $k$.

**Definition**

The *supersingular elliptic rank* $e(A)$ of $A$ is

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

$E_i$ supersingular elliptic curves, $B$ abelian variety of dimension $g - e$, and $\iota$ an isomorphism of abelian varieties.

**Note:** $0 \leq e(A) \leq s(A)$ because each $E_i$ contributes a factor of $E/(F + V)$ to the Dieudonné module

If $A$ absolutely simple, then $e(A) = 0$.

**Lenstra/Oort:** If $\eta$ non-supersingular symmetric formal isogeny type, there exists a simple abelian variety $A$ with isogeny type $\eta$. There are many $A$ with $s(A) > 0$ and $e(A) = 0$. 
An observation of Oort

If $A$ is supersingular, then the supersingular elliptic rank $e(A)$ of $A$ equals the superspecial rank $s(A)$ of $A$.

**Proof sketch:** Know $e \leq s$. Let $E$ be supersingular elliptic curve.

Write $A[p^\infty] \simeq G_{1,1}^s \times Z$ with $s(Z) = 0$. Since $A$ supersingular,

there exists a finite group scheme $N \hookrightarrow G_{1,1}^{g-s}$ s.t. $Z \simeq G_{1,1}^{g-s}/N$.

Now $E^{g-s}$ and $G_{1,1}^{g-s}$ have the same finite subgroup schemes.

So $N \hookrightarrow E^{g-s}$; it follows that $A \simeq E^s \times (E^b/N)$ and $e(A) \geq s$. 
Supersingular, but not superspecial

Proposition - revised
For all $p$ and $g \geq 2$ and $0 \leq s \leq g - 2$, there exists a supersingular abelian variety of dimension $g$ over $\overline{F}_p$ with supersingular elliptic rank $s$.

Thus $A \sim E^g$ with $E$ ss, and $A \simeq B \times (\times_{i=1}^{s} E_i)$ but $A \not\simeq C \times (\times_{i=1}^{s+1} E_i)$.

Question
Given $p$ and $g \geq 2$ and $0 \leq s \leq g - 2$, does there exist a supersingular curve $X$ over $\overline{F}_p$ with genus $g$ whose Jacobian has supersingular elliptic rank $s$?
The Hermitian curve $X_q : y^q + y = x^{q^2+1}$ with $q = p^n$ is supersingular with genus $g = q(q-1)/2$.

**P/Weir:** The distinct indecomposable factors of Dieudonné module $D(X_q)$ are in bijection with orbits of $\mathbb{Z}/(2^n+1) - \{0\}$ under $\times 2$.

Example: $D(X_{p^2}) = (\mathbb{E}/(F^2 + V^2))^{g/2}$.

Check: if $n$ even, then $\mathbb{E}/(F + V)$ is not a factor of $D(X_{p^n})$.

Combinatorial reason: $n$ odd iff there is an element of order three in $\mathbb{Z}/(2^n+1)$ iff there is an orbit of length 2 in $\mathbb{Z}/(2^n+1)$ under $\times 2$.

**Application: P/Weir**

If $n$ is even, the supersingular elliptic rank of $\text{Jac}(X_{p^n})$ equals 0.

If $n$ is odd, the supersingular elliptic rank of $\text{Jac}(X_{p^n})$ equals $(\frac{p(p-1)}{2})^n$. 

---

Pries (CSU)
Let $X$ be a smooth projective curve over $k$.
Let $D(X)$ be the Dieudonné module of the $p$-torsion of $\text{Jac}(X)$.

**Oda:** isomorphism of $\mathbb{E}$-modules between $D(X)$ and $H^1_{dR}(X)$.

**Exact sequence:**

$$0 \to H^0(X, \Omega^1) \to H^1_{dR}(X) \to H^1(X, \mathcal{O}) \to 0.$$ 

Compute the structure of $H^1_{dR}(X)$ under $F$ and $V$.
Write $(f, \omega) \in H^1_{dR}(X)$ where $d\phi = \omega_1 - \omega_2$.
Then $F(f, \omega) := (f^p, 0)$ and $V(f, \omega) := (0, C(\omega))$, where $C$ is the Cartier operator on $\Omega^1$. 
Let $Y$ be a hyperelliptic curve of genus $g$ over $k = \overline{F}_2$. Then $Y : y^2 + y = h(x)$ for some $h(x) \in k(x)$.

**Theorem - Elkin/P**

We determine structure of Dieudonné module of $\text{Jac}(Y)$. It depends only on the orders of the poles of $h(x)$.

E.g., $p$-rank 0 iff $h(x) \in k[x]$ iff the EO type is $[0, 1, 1, 2, 2, \ldots, \lfloor \frac{g}{2} \rfloor]$.

**Application: Elkin/P**

Let $Y$ be a supersingular hyperelliptic curve of genus $g$ over $\overline{F}_2$. Let $e$ be the supersingular elliptic rank of $\text{Jac}(Y)$. Then $e = 1$ when $g \equiv 1 \mod 3$ and $e = 0$ otherwise.

Such curves exist: if $h(x) = xR(x)$ for an additive polynomial $R(x)$ of degree $2^s$, then $Y$ is supersingular of genus $2^{s-1}$ VdG/VdV.
Let $p = 2$, let $q_0 = 2^m$ and let $q = 2^{2m+1}$.

The Suzuki curve $S_q$ has equation $y^q + y = x^{q_0}(x^q + x)$. It is supersingular with genus $q_0(q - 1)$.

**Furlmann/Torres:** $S_q$ is the unique $\mathbb{F}_q$-optimal curve of genus $g$.

**Hansen92:** $S_q$ is the Deligne-Lusztig curve for group $Sz(q) = 2B_2(q)$.

**Application: Malmskog/P/Weir**

The ss-elliptic rank of $\text{Jac}(S_q)$ is 1 when $m$ even and is 0 when $m$ odd.
The Suzuki curve $S_q$ has genus $q_0(q - 1)$ where $q_0 = 2^m$, $q = 2^{2m+1}$.

**Application: Malmskog/P/Weir**

The ss-elliptic rank of $\text{Jac}(S_q)$ is 1 when $m$ even and is 0 when $m$ odd.

**Proof:** Consider tame action of $T \cong \mathbb{Z}/(q - 1)$ on $S_q$.

Giulietti, Korchmaros, Torres: The quotient $S_q / T$ is a supersingular hyperelliptic curve of genus $q_0$. (must also have $p$-rank 0).

Applying Elkin/P to $S_q / T$, the old ss-elliptic rank is 1 when $q_0 \equiv 1 \mod 3$ (even $m$) and is 0 when $q_0 \equiv 2 \mod 3$ (odd $m$).

The new elliptic rank is zero: the orbits of action of $F$ on non-trivial eigenspaces of $H^1_{dR}(S_q)$ are too long.
Supersingular curves with ss-elliptic rank 0 when $p = 2$

**P:** Let $p = 2$. Let $r, s \in \mathbb{N}$ with $s$ even. Let $q = 2^r$.

There exists a supersingular curve $Y$ of genus $g = 2^{s-1}(q - 1)$ with ss-elliptic rank 0.

If $s$ odd, let $\alpha = \text{val}_3(q - 1)$ and $\beta = \text{val}_3(2^s + 1)$.

Then ss-elliptic rank of $Y$ is bounded by $3^\alpha(3^\beta - 1)/2$.

**Proof:** Use VdG/VdV to construct supersingular curve of genus $g$, with automorphism of large prime-to-$p$ order.

*Old* elliptic rank bounded by that of quotient curve.

*New* elliptic rank zero because orbits of action of $F$ on non-trivial eigenspaces of $H^1_{dR}(Y)$ too long.
With Malmskog and Weir, computing the DM of the Suzuki curves.

**Examples** If \( m = 1 \), then \( \text{DM} = \mathbb{E}/(F^2 + V^2) \oplus (\mathbb{E}/(F^3 + V^3))^4 \).

If \( m = 2 \), then \( \text{DM} = \mathbb{E}/(F + V) \oplus \mathbb{E}/(F^3 + V^3) \oplus D^4 \oplus (\mathbb{E}/(F^5 + V^5))^{16} \)

where \( D \) has 3 generators (given by word \( F^{-4} V^3 F^{-3} V^4 F^{-3} V^3 \)).

Strategy: find structure in general using representation theory.
The superspecial rank is an invariant of the DM of abelian variety $A$.

If $A$ supersingular, then it equals the number of superspecial elliptic factors in the decomposition of $A$ up to isomorphism.

Superspecial rank is generically 0 for supersingular abelian varieties.

Expect same is true for supersingular Jacobians of curves.

Questions

1. The supersingular locus $S_g$ of $A_g$ can be stratified by superspecial rank into subspaces $S_{g,s}$.
   For $0 \leq s \leq g - 2$, what is the geometry of $S_{g,s}$?
2. What superspecial ranks occur for supersingular curves?
3. If $A$ supersingular, understand connection between superspecial rank and properties of the isogeny $A \sim E^g$.

Thanks!