

Open questions on Jacobians of curves over finite fields: supersingular curves

Rachel Pries

Colorado State University
pries@math.colostate.edu

Effective methods for abelian varieties
June 16-18, 2016

Open question on supersingular curves

Let p be a prime number. Let g be a natural number.

Open question:

Does there exist a supersingular curve of genus g defined over a finite field of characteristic p , for every p and g ?

Outline. What is:

- 1 a supersingular elliptic curve;
- 2 a supersingular curve of higher genus;
- 3 known about this question already;
- 4 the next step?

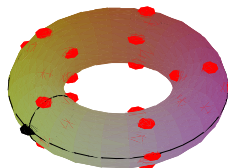
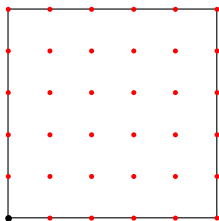
Complex elliptic curves and p -torsion

Let E be a complex elliptic curve.

$E \simeq \mathbb{C}/L$ for a lattice $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.
(Thus E is an abelian group).

Torsion points: $E[p](\mathbb{C}) = \{Q \in E(\mathbb{C}) \mid pQ = 0_E\}$.

Then $E[p](\mathbb{C}) \simeq \frac{1}{p}L/L \simeq (\mathbb{Z}/p)^2$.

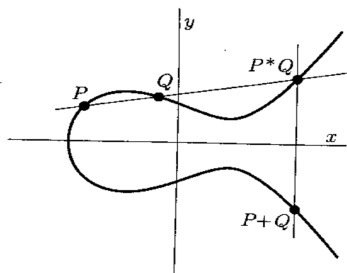


If X is a complex curve of genus $g \geq 2$, its Jacobian J_X is a p.p. abelian variety of dimension g and $J_X[p](\mathbb{C}) \simeq (\mathbb{Z}/p)^{2g}$.

Elliptic curves - algebraic version

Let $E : y^2 = h(x)$ be an elliptic curve over $k = \overline{\mathbb{F}}_p$ where $h(x) = x^3 + ax^2 + bx + c = \prod_{i=1}^3 (x - \lambda_i)$.

Algebraic group law on E :



The ℓ -torsion of E is $\text{Ker}[\ell]$ where $[\ell] : E \rightarrow E$ is mult.by- ℓ .

$$E[\ell](k) := \{Q \in E(k) \mid \ell Q = 0_E\} \simeq (\mathbb{Z}/\ell)^2 \text{ if } p \nmid \ell.$$

Torsion points - example

Let $E : y^2 = x^3 + ax^2 + bx + c$ and $\ell = 3$.

A point Q has order 3 iff $2Q = -Q$ iff $x(2Q) = x(Q)$.

This occurs iff $x(Q)$ is a root of the 3-division polynomial.

$P. < a, b, c > = \text{PolynomialRing}(\mathbb{Z}, 3)$

$E = \text{EllipticCurve}(P, [0, a, 0, b, c])$

$d_3 = E.\text{division_polynomial}(3, x = \text{None})$

$$3 * x^4 + 4 * a * x^3 + 6 * b * x^2 + 12 * c * x - b^2 + 4 * a * c$$

If $p \neq 3$, then $d_3(x)$ has 4 distinct roots so E has 8 points of order 3 and $|E[3](k)| = 9$.

Collapsing torsion points - example

What if $p = 3$?

$$d_3 = 3 * x^4 + 4 * a * x^3 + 6 * b * x^2 + 12 * c * x - b^2 + 4 * a * c.$$

Collapsing torsion points - example

What if $p = 3$?

$$d_3 = 3 * x^4 + 4 * a * x^3 + 6 * b * x^2 + 12 * c * x - b^2 + 4 * a * c.$$

$P_3. \langle a, b, c \rangle = \text{PolynomialRing}(GF(3), 3)$

$r_3 = d_3.\text{change_ring}(P_3)$

$$+ a * x^3 - b^2 + a * c$$

Mod p binomial thm: In $k[x]$, $(x + \alpha)^p = x^p + \alpha^p$.

So $r_3 = a * x^3 - b^2 + a * c$ has

$$\begin{cases} \text{one (triple) root} & a \not\equiv 0 \pmod{3} \\ \text{no roots} & a \equiv 0 \pmod{3} \end{cases}$$

So $|E[3](k)|$ divides 3 when $p = 3$.

Ordinary and supersingular elliptic curves

p	r_p reduction of p -division polynomial of $y^2 = x^3 + bx + c$
5	$+2 * b * x^{10} - b^2 * c * x^5 + b^6 - 2 * b^3 * c^2 - c^4$
7	$+3 * c * x^{21} + 3 * b^2 * c^2 * x^{14} + (-b^7 * c - 2 * b^4 * c^3 + 3 * b * c^5) * x^7 - b^{12} - b^9 * c^2 + 3 * b^6 * c^4 - b^3 * c^6 + 2 * c^8$

Then r_p has at most $(p-1)/2$ roots. The p -torsion points on $E : y^2 = f(x)$ collapse to either p points or 1 point modulo p .

Def:

$$E \text{ is } \begin{cases} \text{ordinary} & \text{if } |E[p](k)| = p \\ \text{supersingular} & \text{if } |E[p](k)| = 1 \end{cases}$$

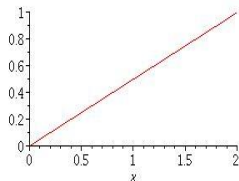
Supersingularity and slopes

If E/\mathbb{F}_q is elliptic curve, then $\#E(\mathbb{F}_q) = q + 1 - a$.

The zeta function of E is $Z(t) = (1 - at + qt^2)/(1 - t)(1 - qt)$.

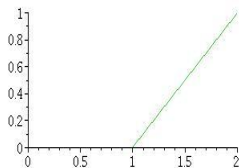
Fact: $p \mid a$ iff E supersingular.

E supersingular, Newton polygon of $1 - at + qt^2$ has slopes $1/2$.



called $G_{1,1}$.

E ordinary, then Newton polygon has slopes 0 and 1.



called $G_{0,1} \oplus G_{1,0}$.

```
E = EllipticCurve(GF(5), [0, 1, 0, 2, 0])
```

Elliptic Curve defined by $y^2 = x^3 + x^2 + 2 * x$ over Finite Field of size 5

```
E.is_supersingular()
```

True

```
E.hasse_invariant()
```

0

```
E.trace_of_frobenius()
```

0

```
F = E.frobenius()
```

```
C = F.absolute_charpoly()
```

$x^2 + 5$

```
C.newton_slopes(5)
```

$[1/2, 1/2]$

Examples of supersingular elliptic curves

For all p , there exists a supersingular elliptic curve E/\mathbb{F}_{p^2} (Igusa).

The number of isomorphism classes of ss elliptic curves is $\lfloor \frac{p}{12} \rfloor + \varepsilon$.

$p = 2$: $y^2 + y = x^3$ (unique)

$p \equiv 3 \pmod{4}$: $y^2 = x^3 - x$

$p \equiv 2 \pmod{3}$: $y^2 = x^3 + 1$

p odd: $y^2 = h(x)$, where $h(x)$ cubic with distinct roots, is supersingular iff the coefficient c_{p-1} of x^{p-1} in $h(x)^{(p-1)/2}$ is zero.

This coefficient vanishes iff Cartier operator trivializes $\frac{dx}{y} \in H^0(E, \Omega^1)$.

$$C\left(\frac{dx}{y}\right) = C\left(\frac{y^{p-1} dx}{y^p}\right) = \frac{1}{y} C(h(x)^{(p-1)/2}) dx = \frac{c_{p-1}^{1/p} dx}{y}.$$

$y^2 = x(x-1)(x-\lambda)$ is supersingular for $\frac{p-1}{2}$ choices of $\lambda \in \overline{\mathbb{F}}_p$ (Igusa).

Review: supersingular elliptic curves

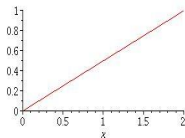
Let E be a smooth elliptic curve over $k = \bar{k}$, with $\text{char}(k) = p$.

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 Cartier operator annihilates $H^0(E, \Omega^1)$.

D. $\text{End}(E)$ non-commutative (order in quat. algebra)

Introduction: different properties when $g > 1$

Let A be a p.p. abelian variety of dimension g over $k = \bar{k}$, $\text{char}(k) = p$.
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 Cartier operator annihilates $H^0(X, \Omega^1)$.

Then $C \Rightarrow B \Rightarrow A$ but $A \stackrel{g \geq 3}{\not\Rightarrow} B \stackrel{g \geq 2}{\not\Rightarrow} C$

Question: if $g \geq 2$, do these occur for Jacobian of smooth k -curve?

Curves of higher genus

Let $k = \overline{\mathbb{F}}_p$ (an algebraically closed field of char. p).

Let X be a (smooth projective connected) curve over k .

Recall: everything you learned about Riemann surfaces (\mathbb{C} -curves).

Analogous structures: e.g., functions, differentials, Jacobians.

More complicated definitions: e.g., genus is $g = \dim(H^0(X, \Omega_1))$ rather than 'the number of holes'.

Guideline:

Most facts not involving the number p are still true.

Most facts involving the number p are now false.

Suppose X is a curve. The genus is $g = \dim(H^0(X, \Omega_1))$.

If $g \geq 2$, there is no natural group law on the points of X .

(Recall, define group structure on points of a complex curve by integrating holomorphic differentials and taking quotient by lattice of periods: $J_X = \Omega^1(X)^* / H^1(X, \mathbb{Z}) \simeq \mathbb{C}^g / \mathbb{L}$. Its p -torsion points satisfy $J_X[p](\mathbb{C}) \simeq (\mathbb{Z}/p)^{2g}$.)

Now Jacobian J_X of X is $\text{Pic}^0(X)$ (line bundles of deg 0) or $\text{Div}^0(X)/\text{PDiv}(X)$ (divisors of deg 0 mod principal divisors).

Then J_X is a principally polarized abelian variety of dimension g .

B. Definition of Newton polygon

Let X be a smooth projective curve defined over \mathbb{F}_q , with $q = p^a$.
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 λ occurs with length m_λ , 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 $1/2$.

B. Definition of Newton polygon

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_λ for $G_{c,d}$ is a $W(k)$ -module.

Over $\text{Frac}(W(k))$, there is a basis x_1, \dots, x_d for D_λ 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 slope λ , length m_λ .

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

There is a partial ordering on NPs; the supersingular NP is 'smallest'.

The supersingular property

Let X be a smooth projective curve defined over \mathbb{F}_q , with $q = p^a$.
The following are equivalent:

- 1 X is supersingular;
- 2 the Newton polygon of $L(X/\mathbb{F}_q, T)$ is a line segment of slope $1/2$;
- 3 each eigenvalue of the relative Frobenius morphism equals $\zeta\sqrt{q}$ for some root of unity ζ ;
- 4 X is minimal (satisfies lower bound in Hasse-Weil bound for number of points) over \mathbb{F}_{q^r} for some r ;
- 5 Tate: $\text{End}(\text{Jac}(X \times_{\mathbb{F}_q} k)) \otimes \mathbb{Q}_p \simeq M_g(D_p)$, D_p quat alg ram at p , ∞ ;
- 6 Oort: $\text{Jac}(X)$ is geometrically isogenous to a product of supersingular elliptic curves.

Motivation for studying supersingular curves

- * maximal and minimal curves (supersingular) yield good error-correcting Goppa codes;
- * abelian varieties with complex multiplication are often supersingular, useful in cryptography;
- * good signature schemes built using supersingular curves;
- * supersingular curves play a key role in geometric proofs about stratifications of \mathcal{A}_g by Newton polygon type (or EO type).

Example: Hermitian curves are supersingular

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 L -polynomial of X_q is $L(X_q/\mathbb{F}_q, t) = (1 + qt^2)^g$.

The only slope of the Newton polygon of $L(X_q/\mathbb{F}_q, t)$ is $1/2$.

Thus $\text{Jac}(X_q)$ is supersingular.

Which Newton polygons occur for Jacobians?

For all p and g , there exists:

a supersingular p.p. *abelian variety* of dimension g , namely E^g ;
and a supersingular *singular curve* of genus g .

Open question:

Does there exist a supersingular smooth curve of genus g defined over a finite field of characteristic p , for every p and g ?

More generally,

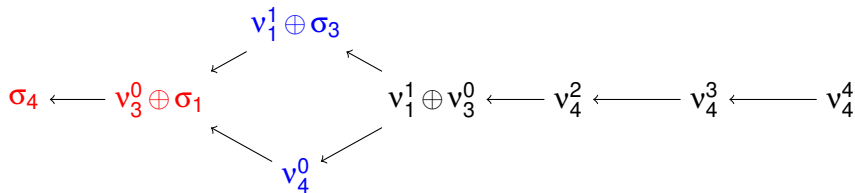
which Newton polygons occur for Jacobians of smooth curves?

For $g = 1$ both, $g = 2$ all three, $g = 3$ all five.

Let \mathcal{A}_g be the moduli space of p.p. abelian varieties of dimension g .
The image of \mathcal{M}_g in \mathcal{A}_g is open and dense for $g \leq 3$.

Open question for $g = 4$:

For all p , does there exist a smooth curve of genus 4 which is supersingular? or whose NP has slopes $1/3, 1/2, 2/3$?



- *: don't know if this NP occurs for Jacobian of smooth curve for all p
- *: this NP occurs but some components may have problems
- *: each component has good geometric properties.

(Katz, Oort, Faber/Van der Geer, Pries, Achter-Pries)

Do all NPs occur for Jacobians? Guess - unlikely?

Observation (Oort 2005) $\dim(\mathcal{A}_g) = g(g+1)/2$ and the dimension of the supersingular locus $\mathcal{A}_g[\sigma_g]$ is $\lfloor g^2/4 \rfloor$.

The difference δ_g is length of longest chain of NPs connecting the supersingular NP σ_g to the ordinary NP ν_g .

If $g \geq 9$, then $\delta_g > 3g - 3 = \dim(\mathcal{M}_g)$.

Either (i) \mathcal{M}_g does not admit a perfect stratification by NP (i.e., there are two NPs ξ_1 and ξ_2 such that $\mathcal{A}_g[\xi_1]$ is in the closure of $\mathcal{A}_g[\xi_2]$ but $\mathcal{M}_g[\xi_1]$ is not in the closure of $\mathcal{M}_g[\xi_2]$.)

or (ii) some NPs do not occur for Jacobians of smooth curves.

Test case: $g = 11$ with NP $G_{5,6} \oplus G_{6,5}$ having slopes of $5/11, 6/11$ (does occur when $p = 2$ - Blache).

Do all NPs occur for Jacobians? Evidence?

Only non-existence results are for curves with automorphisms:

Bouw 2001: Not all p -ranks occur for cyclic degree $d > 2$ covers

Especially, not all NPs occur for wildly ramified covers:

Deuring-Shafarevich formula restricts p -rank.

Oort: If $p = 2$, there does not exist a hyp. ss curve of genus 3.

Scholten/Zhu: $p = 2$, $n \geq 2$, there is no hyp. ss curve with $g = 2^n - 1$.

(for odd p , generalized for Artin-Schreier covers $X \xrightarrow{\mathbb{Z}/p} \mathbb{P}^1$ by Blache)

But.....

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

Step one of proof by VdG/VdV

Def: $R[x] \in k[x]$ is an additive polynomial if $R(x_1 + x_2) = R(x_1) + R(x_2)$.
Then $R[x] = c_0x + c_1x^p + c_2x^{p^2} + \dots + c_hx^{p^h}$.

Supersingular Artin-Schreier curves

If $R[x] \in k[x]$ is an additive polynomial of degree p^h , then $X : y^p - y = xR[x]$ is supersingular with genus $p^h(p-1)/2$.

Proof: Induction on h , starting with $h = 0$.

Key fact: $\text{Jac}(X)$ is isogenous to a product of Jacobians of Artin-Schreier curves for additive polynomials of smaller degree.

Remark: Bouw et al studied L -polynomials, automorphism groups of X .

Remark: Blache studied first slope of NP of more general AS curves

Existence of supersingular curves when $p = 2$

Van der Geer and Van der Vlugt

If $p = 2$, then there exists a supersingular curve over $\overline{\mathbb{F}}_2$ of every genus.

Proof sketch: Expand g as (with $s_i \leq s_{i-1} + r_{i-1} + 2$)

$$g = 2^{s_1}(1 + 2 + \cdots + 2^{r_1}) + 2^{s_2}(1 + 2 + \cdots + 2^{r_2}) + \cdots + 2^{s_t}(1 + 2 + \cdots + 2^{r_t}).$$

Let $\mathbf{L} = \bigoplus_{i=1}^t L_i$ for L_i subspace of dim $d_i := r_i + 1$ in vector space of additive polynomials of deg 2^{u_i} , with $u_i = (s_i + 1) - \sum_{j=1}^{i-1} (r_j + 1)$.

If $f \in \mathbf{L}$, let $C_f : y^p - y = xf$. Let Y be fiber product of $C_f \rightarrow \mathbb{P}^1$ for all $f \in \mathbf{L}$. Then $J_Y \sim \bigoplus_{f \neq 0} J_{C_f}$ (thus supersingular). Also, $g_Y = \sum_{f \neq 0} g_{C_f}$.

The number of $f \in \mathbf{L}$ which have a non-zero contribution from L_i , but not from L_j for $j > i$, is $(2^{d_i} - 1) \prod_{j=1}^{i-1} 2^{d_j}$. Each adds 2^{u_i-1} to g .

$$\text{So } g_Y = \sum_{i=1}^t (2^{d_i} - 1) \prod_{j=1}^{i-1} 2^{d_j} 2^{u_i-1} = \sum_{i=1}^t 2^{s_i} (1 + \cdots + 2^{r_i}) = g.$$

Supersingular Artin-Schreier curves for odd p

Here is what VdG/VdV's method produces for odd p .

Karemaker/P

Let $g = Gp(p-1)^2/2$ where $G = \sum_{i=1}^t p^{s_i}(1+p+\dots+p^{r_i})$. Then there exists a supersingular curve over $\overline{\mathbb{F}}_p$ of genus g .

Can this be improved?

VdG/VdV also prove that there exists a supersingular curve defined over \mathbb{F}_2 of every genus. The construction is a little more complicated.

Related question: the p -rank of X

If X is a smooth k -curve of genus g ,

Fact/Def:

then $|J_X[p](k)| = p^f$ for some integer $0 \leq f \leq g$ called the p -rank of X .

Also, $f = \dim_{\mathbb{F}_p} \text{Hom}(\mu_p, J_X[p])$ where $\mu_p \simeq \text{Spec}(k[x]/(x^p - 1))$ is the kernel of Frobenius on \mathbb{G}_m .

Let $L(t)$ be the L -polynomial of the zeta function of an \mathbb{F}_q -curve X .

The p -rank of X is the length of the slope 0 portion of $\text{NP}(X)$.

X is supersingular if all slopes of $\text{NP}(X)$ equal $1/2$.

X supersingular implies X has p -rank 0 but converse false for $g \geq 3$.

Existence of curves with given genus and p -rank

Let $g \in \mathbb{N}$, $0 \leq f \leq g$ and p prime.

The moduli space \mathcal{M}_g (resp. \mathcal{H}_g) of (hyperelliptic) curves of genus g can be stratified by p -rank into strata \mathcal{M}_g^f (resp. \mathcal{H}_g^f) whose points represent (hyperelliptic) curves of genus g and p -rank f .

Theorem: Faber/Van der Geer

Every component of \mathcal{M}_g^f has dimension $2g - 3 + f$;
there exists a smooth curve over $\overline{\mathbb{F}}_p$ with genus g and p -rank f .

Theorem: Glass/P (p odd), P/Zhu (p even)

Every component of \mathcal{H}_g^f has dimension $g - 1 + f$;
there exists a smooth hyp. curve over $\overline{\mathbb{F}}_p$ with genus g and p -rank f .

In most cases, it is not known whether \mathcal{M}_g^f and \mathcal{H}_g^f are irreducible.

Supersingular versus p -rank 0

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

Fact: If A is supersingular, then A has p -rank 0.

If $g \in \{1, 2\}$ and A has p -rank 0, then A is supersingular.

If $g \geq 3$ and A has p -rank 0, then A usually not supersingular.

Example: Let $j \in \mathbb{N}$ with $p \nmid j$ and $h(x) \in k[x]$ of degree j .
The curve $X : y^q + y = h(x)$ has genus $g = (q-1)(j-1)/2$.
Deuring-Shafarevich formula: $\text{Jac}(X)$ has p -rank 0.

Zhu: Let $q = 2$ and $j = 2^{n+1} - 1$, none of the 2-rank 0 curves $y^2 + y = h(x)$ are supersingular.

Moduli of curves: supersingular versus p -rank 0

Oort: There exists a hyperelliptic curve of genus 3 with p -rank 0 which is not supersingular.

proof: study intersection of two codim 1 conditions in \mathcal{M}_3^0 .

Application - Achter/P. Let $g \geq 3$ and $p \neq 2$ for hyperelliptic

The generic point of any component of the p -rank 0 strata \mathcal{M}_g^0 and \mathcal{H}_g^0 is not supersingular.

$A \not\Rightarrow B$ for curves:

if $g \geq 3$, there exists a (hyperelliptic) curve of genus g with p -rank 0 which is not supersingular.

Newton polygon results for $f = g - 3$ and $f = g - 4$

For $g \geq 4$ and $g - 2 \leq f \leq g$, the p -rank determines the Newton polygon (and so that Newton polygon occurs, open and dense in \mathcal{M}_g^f).

Let $v_{g,f} = f(G_{0,1} + G_{1,0}) + (G_{1,g-f-1} + G_{g-f-1,1})$.

Application - Achter/P. Let $g \geq 3$ and $f = g - 3$.

The generic point of each component of \mathcal{M}_g^{g-3} has Newton polygon $v_{g,g-3}$ (slopes $0, \frac{1}{3}, \frac{2}{3}, 1$).

Application - Achter/P. Let $g \geq 4$ and $f = g - 4$.

The generic point of *at least one* component of \mathcal{M}_g^f has Newton polygon $v_{g,g-4}$ (slopes $0, \frac{1}{4}, \frac{3}{4}, 1$).

Note: When $g = 4$, there is *at most one* component of \mathcal{M}_4^0 whose generic NP is not $v_{4,0}$. If so, the NP has slopes $\frac{1}{3}, \frac{1}{2}, \frac{2}{3}$.

Proof: inductive strategy, reduce to p -rank $f = 0$

Let v_r be a NP type with p -rank 0 occurring in dimension r .

Let $c_r = \text{codim}(\mathcal{A}_g[v_r], \mathcal{A}_g)$.

For $g \geq r$, let v_g be the NP type with p -rank $g - r$ 'containing' v_r

($v_g = (G_{0,1} \oplus G_{1,0})^{g-r} \oplus v_r$), add $g - r$ slopes of 0, 1.

Proposition P

If there exists a component S_r of $\mathcal{M}_r[v_r]$ s.t. $\text{codim}(S_r, \mathcal{M}_r) = c_r$,

then, for all $g \geq r$,

there exists a component S_g of $\mathcal{M}_g[v_g]$ s.t. $\text{codim}(S_g, \mathcal{M}_g) = c_r$.