A Magma Package for Classifying and Computing p-torsion Varieties

Colin Weir

Tutte Institute for Mathematics and Computing

Joint work with Mark Bauer - University of Calgary

December 2018

Are you tired of working in characteristic 0?

Looking for something more?

Considering p-torsion

Let k be an algebraically closed field in characteristic p.
Let X be an (adjectives) curve over a field k of genus g.
Its Jacobian J_X is a p.p. abelian variety of dimension g.

When $\ell \neq p$:

$J_X[\ell](k) := Ker[\ell] \cong (\mathbb{Z}/\ell)^{2g}$.

When $\ell = p$:

Considering p-torsion

Let k be an algebraically closed field in characteristic p.
Let X be an (adjectives) curve over a field k of genus g.
Its Jacobian J_X is a p.p. abelian variety of dimension g.

When $\ell \neq p$:

$J_X[\ell](k) := Ker[\ell] \cong (\mathbb{Z}/\ell)^{2g}$.

When $\ell = p$:

$J_X[p](k) \cong (\mathbb{Z}/p)^f$ for some $0 \leq f \leq g$.

In characteristic p, multiplication by p is inseparable.

Market research on inseparability:

Market research on inseparability:

- "Inseparability is Galois cruelty!"
  — An undergraduate

Market research on inseparability:

- "Inseparability is Galois cruelty!"
  — An undergraduate
- "That is interesting! Tell me more about $J_X[p]$!"
  — A mathematician

Market research on inseparability:

- "Inseparability is Galois cruelty!"
  — An undergraduate
- "That is interesting! Tell me more about $J_X[p]$!"
  — A mathematician
- "Inseparability is used in marketing to describe a key quality of services as distinct from goods."
  — Wikipedia

Inseparability

Market research on inseparability:

- "Inseparability is Galois cruelty!"
  — An undergraduate
- "That is interesting! Tell me more about $J_X[p]$!"
  — A mathematician
- "Inseparability is used in marketing to describe a key quality of services as distinct from goods."
  — Wikipedia

We're talking about computing inseparability like never before!!!

p-torsion Group Schemes in General

Let $A[p]$ be a finite group scheme annihilated by p, with two morphisms, the Frobenius F and the Verschiebung V (F's dual) where

$$[p] = F \circ V,$$

How many isomorphism types have rank p^{2g}?

p-torsion Group Schemes in General

Let $A[p]$ be a finite group scheme annihilated by p, with two morphisms, the Frobenius F and the Verschiebung V (F's dual) where

$$[p] = F \circ V,$$

How many isomorphism types have rank p^{2g}?

Definition

There exists a filtration $N_1 \subset N_2 \subset \cdots \subset N_{2g} = A[p]$ stable under V and F^{-1}, such that $\dim_k(N_i) = i$. Set $v_i := \dim_k(VN_i)$.
The Ekedahl - Oort type is $v := [v_1, \ldots, v_g]$.

- It is nec/suff that $v_i \leq v_{i+1} \leq v_i + 1$.
- EO-types uniquely detemine isomorphism classes.
- Thus there are 2^g possibilities for $J_X[p]$.
- Given F & V, just iterate $F^{-j}(\mathrm{Im}(V^i))$ to compute the N's.

New this holiday season… p-torsion group schemes in Magma!!!

Isomorphic Viewpoints

We use the follow equivalences:

BT-1 groups schemes of rank p^{2g}

$J_X[p]$ is one of these.

$\updownarrow$

Dieudonné modules of dim $2g$ (mod p)

Module over $\mathbb{E}$ generated by F and V such that $FV = VF = 0$.

$\updownarrow$

$H^1_{dR}(X)$ with F,V actions

'Concrete' vector space with explicit actions.

Computing with $H^1_{dR}(X)$

In General:

$$0 \to H^0(X, \Omega_1) \to H^1_{dR}(X) \to H^1(X, \mathcal{O}) \to 0$$

The Algorithm Outline:

- This sequence is non-split as F, V modules.
- Compute bases of $H^0(X, \Omega_1)$ and $H^1(X, \mathcal{O})$.
- Compute F and V on $H^1(X, \mathcal{O})$ and $H^0(X, \Omega_1)$.
- 'Extend' F & V to putative actions on $H^1_{dR}(X)$.
- Iterate F^{-1} and V to compute the EO-type.

Notation:

- Let K be the function field of the curve X of genus g.
- Assume K has exact constant field $k = GF(q) = GF(p^n)$.
- Let $d = [K : k(x)]$.

Example Magma:

```
> EOType(K);
[0,1,1]
```

Runtime:

$$\begin{array}{rcccccc} & \tilde{O}(& q(gd)^2 & + & p(gn)^3 & + & (png)^3 &) \\ = & \tilde{O}(& \text{R.R. Bases} & + & \text{Lin Alg} & + & \text{Reductions} &) \end{array}$$

NOTE: Asympototics were sacrificed for practical performance.

Now with all new features!!

Isomorphic Viewpoints

Recall the follow equivalences:

BT-1 groups schemes of rank p^{2g}

$J_X[p]$ is one of these.

$\updownarrow$

Dieudonné modules of dim $2g$ (mod p)

Module over $\mathbb{E}$ generated by F and V such that $FV = VF = 0$.

$\updownarrow$

$H^1_{dR}(X)$ with F,V actions

'Concrete' vector space with explicit actions.

EO-Type to Dieudonné Modules

- There is a canonical choice of F and V actions (over $GF(p)$) for each EO-type.

Example Magma:

```
> FVModule([0,0,1], p);
K-module of dimension 6 over GF(p)
```

- We can decompose the Dieudonné module and ask for the relations for each component.

Example Magma:

```
> PrintFVRelations([1,1,1]);
 {* [F], [V], [F + V]^^2] *}
```

That's not all!

There's more!!

EO-Type to Permutations

- Recall the filtration $N_1 \subset N_2 \subset \cdots \subset N_{2g} = A[p]$
- F^{-1}, V act as a permutation on $\{N_{i+1}/N_i\}$.
- The cycle decomposition gives the decomposition of the Dieudonné module!
- You can read off this permutation from the EO-type!

Example Magma:

```
> EOTypeToPermutation([0,1,1]);
(1,4,2)(3,5,6)
```

Example Magma:

```
> PermutationToEOType([ 4, 1, 5, 2, 6, 3 ]);
 [0,1,1]
```

Composing and Decomposing

- Using the above methods we do products and decomposition in $\tilde{O}(g)$ time!
- Just map EO-types to permutations and then map cycles back to EO-types.

Example Magma:

```
> DecomposeEO([0,1,1]);)
 {* [ 0 ], [ 1 ], [ 0, 1 ]^^2 *}
```

Example Magma:

```
> ComposeEO({* [ 0 ], [ 1 ], [ 0, 1 ]^^2 *});
 [0, 1, 1]
```

NOTE: PrintFVRelations actually calls these functions instead of decomposing the module with Magma.

Looking for an EO-type for that special someone?

Prym varieties are now available!!!

- Let $C \to D$ be an unramified double cover.
- Then $J_C \cong J_D \oplus \mathrm{Prym}_{C/D}/H$ where H is a 2-group.
- Thus in, characteristic p > 2

$$J_C[p] \cong J_D[p] \oplus \mathrm{Prym}_{C/D}[p]$$

If $dim(J_D) = g$ then $dim(J_C) = 2g + 1$ and $dim(\mathrm{Prym}_{C/D}) = g - 1$.

We can simply compute the EO-type of $\mathrm{Prym}_{C/D}$ as

Example Magma:

```
> EOPrym:=ComposeEO(
Decompose(EOType(C)) diff Decompose(EOType(D))
);
```

Computing the EO-type of Pryms:

	$q = 5^2$, $g = 4$	$q = 23$, $g = 4$	$q = 3$, $g = 10$	$q = 3$, $g = 15$
Avg HE Curve EO	0.073	2.796	0.139	0.288
Avg Cover EO	0.329	13.088	0.671	1.460
Avg Prym EO	0.001	0.001	0.003	0.004
Avg C/D	0.936	14.876	1.039	2.078

Computing the EO-type of Hyperelliptic Curves:

	$q = 51$, $g = 5$	$q = 5$, $g = 51$	$q = 17$, $g = 11$	$q = 11$, $g = 17$
Avg HE Curve EO	25.254	11.098	16.847	16.591

For 3 EASY downloads of 19.99 KB you too can have this amazing new package!!

Thank you