Automorphism groups, elliptic curves, and the PORC conjecture

Mima Stanojkovski, joint with C. Voll

Max-Planck-Institut für
Mathematik
in den Naturwissenschaften

Bar-Ilan University Algebra Seminar

4th November 2020

MAX-PLANCK-GESELLSCHAFT

Theorem (S-Voll, 2020+)

Let E be an elliptic curve over $\mathbb{Q}$ and let $\mathbb{F}$ be a finite field of odd characteristic p over which E has good reduction. Assume, moreover, that $|E[2](\mathbb{F})| = 4$. Then there exist groups $\mathbf{G}_1(\mathbb{F})$, $\mathbf{G}_2(\mathbb{F})$, and $\mathbf{G}_3(\mathbb{F})$ satisfying:

- *for each $i = 1, 2, 3$, there exists $T_i \leq E \rtimes \mathrm{Aut}(E)$ such that*

$$|\operatorname{Aut} \mathbf{G}_i(\mathbb{F})| = |\mathbb{F}|^{18} \cdot |\operatorname{GL}_2(\mathbb{F})| \cdot |T_i(\mathbb{F})| \cdot |\operatorname{Gal}(\mathbb{F}/\mathbb{F}_p)|;$$

- *if $\delta \in \mathbb{Z} \setminus \{0\}$ and E is given by $y^2 = x^3 - x/\delta$, then*

$$T_i = E[3] \rtimes \mathrm{Aut}(E)[\lceil 4/i \rceil];$$

- *any two δ's modulo p yield 4 or 6 pairwise non-isomorphic groups of order $|\mathbb{F}|^9$, exponent p, and nilpotency class 2.*

Today on the menu:

- Connection to counting p-groups and the PORC conjecture
- Computational evidence and a motivating example
- The construction of the three groups from determinantal representations of E
- Automorphisms of E vs. automorphisms of $\mathbf{G}$
- Many other comments and questions

COUNTING p-GROUPS

Formulas, asymptotics, and the PORC conjecture

$\Pi = \{\text{prime numbers}\}$

Let $f : \Pi \times \mathbb{Z}_{>0} \to \mathbb{Z}$ be the function

$$(p, n) \mapsto f(p, n) = \#\{ \text{ groups of order } p^n\}/\cong .$$

$\Pi = \{\text{prime numbers}\}$

Let $f : \Pi \times \mathbb{Z}_{>0} \to \mathbb{Z}$ be the function

$$(p, n) \mapsto f(p, n) = \#\{\text{ groups of order } p^n\}/\cong .$$

1. $f(p, 1) = 1$
2. $f(p, 2) = 2$
3. $f(p, 3) = 5$

$\Pi = \{\text{prime numbers}\}$

Let $f : \Pi \times \mathbb{Z}_{>0} \to \mathbb{Z}$ be the function

$$(p, n) \mapsto f(p, n) = \#\{\text{ groups of order } p^n\}/\cong .$$

1. $f(p, 1) = 1$
2. $f(p, 2) = 2$
3. $f(p, 3) = 5$
4. $f(p, 4) = \begin{cases} 14 & \text{if } p = 2, \\ 15 & \text{otherwise.} \end{cases}$
5. $f(p, 5) = \begin{cases} 51 & \text{if } p = 2, \\ 67 & \text{if } p = 3, \\ 2p + 2\gcd(p-1, 3) + \gcd(p-1, 4) + 61 & \text{if } p \geq 5. \end{cases}$

Known values of $f(p,n)$: $n \in \{1,\ldots,7\}$.

Work of authors like Hölder, Hall, Senior, Bender, James, Newman, O'Brien, Eick, Vaughan-Lee and many others ...

Higman and Sims: asymptotic behaviour

$$\lim_{n\to\infty} f(p,n) = p^{\left(\frac{2}{27}+o(1)\right)n^3}.$$

Higman's PORC conjecture: for each positive integer n, there exists a positive integer N and polynomials

$$f_0,\ldots,f_{N-1} \in \mathbb{Z}[x]$$

such that

$$p \equiv i \bmod N \implies f(p,n) = f_i(p).$$

1. $f(p,1) = 1$ (N=1)
2. $f(p,2) = 2$ (N=1)
3. $f(p,3) = 5$ (N=1)
4. $f(p,4) = \begin{cases} 14 & \text{if } p = 2, \\ 15 & \text{otherwise.} \end{cases}$ (N=2)
5. $f(p,5) = \begin{cases} 51 & \text{if } p = 2, \\ 67 & \text{if } p = 3, \\ \tilde{f}(p, \gcd(p-1,3), \gcd(p-1,4)) & \text{if } p \geq 5. \end{cases}$ (N=12)
6. $f(p,6)$ (N=60)
7. $f(p,7)$ (N=2520)

Many counting results for p-groups build upon the p-group generation algorithm of Newman and O'Brien.

Let p be a prime and G a finite p-group.

- The lower p-central series of G is

$$P_1(G) = G \text{ and } P_{i+1}(G) = [G, P_i(G)]P_i(G)^p.$$

- An immediate descendant of G is an extension

$$1 \to P_c(E) \to E \to G \to 1$$

  satisfying $P_c(E) \neq 1$ and $P_{c+1}(E) = 1$.

The automorphism group $\mathrm{Aut}(G)$ of G plays an important role in the determination of the isomorphism types of the immediate descendants of G.

GROUPS AND ALGEBRAS FROM MATRICES OF FORMS

A general construction for class at most 2

- $R = \mathcal{O}_k$ ring of integers of a number field k
- K field with R-algebra structure (for us: K/k or $K = R/\mathfrak{m}$)
- $d \in \mathbb{Z}_{>0}$ and $U, W, T \cong K^d$ vector spaces
- $\mathrm{B} = \mathrm{B}(\mathbf{y}) \in \mathrm{Mat}_d(R[y_1, \ldots, y_d])$ matrix of linear forms, i.e.

$$\mathrm{B}(\mathbf{y}) = \mathrm{B}^{(1)}\, y_1 + \ldots + \mathrm{B}^{(d)}\, y_d \text{ with } \mathrm{B}^{(k)} \in \mathrm{Mat}_d(R)$$

- $\phi : U \times W \to T$ bilinear given by $(u, w) \mapsto u\,\mathrm{B}\,w^{\mathrm{t}}$

Example. If $U = W = T = K^2$ and $\mathrm{B} = \mathrm{diag}(y_1, y_2)$, then

$$\begin{aligned}\phi(u, w) &= (u_1, u_2) \begin{pmatrix} y_1 & 0 \\ 0 & y_2 \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \\ &= u_1 w_1 e_1 + u_2 w_2 e_2 = (u_1 w_1, u_2 w_2).\end{aligned}$$

On the set $L = U \oplus W \oplus T$ define

- a group $\mathrm{G} = \mathbf{G}_{\mathrm{B}}(K) = (L, \star)$ by

$$(u, w, t) \star (u', w', t') = (u + u', w + w', t + t' + \phi(u, w'))$$

- a K-Lie algebra $\mathfrak{g} = \mathfrak{g}_{\mathrm{B}}(K) = (L, [\ ,\ ])$ by

$$[(u, w, t), (u', w', t')] = \phi(u, w') - \phi(u', w) \in T$$

Example.

- $\mathrm{B} = 0 \iff \mathrm{G}$ and $\mathfrak{g}$ abelian
- if $\mathrm{B} = (y_1)$, then $\mathrm{G} \cong \mathrm{Heis}(K)$ and $\mathfrak{g} \cong \mathfrak{heis}(K)$.
- if $K = \mathbb{F}_p$ and p odd, then $|\mathrm{G}| = p^{3d}$ and $\exp(\mathrm{G}) = p$.

Recall $L = U \oplus W \oplus T$ and $\phi : U \times W \to T$

Identities in the group

- $\mathrm{id} = (0, 0, 0)$
- $(u, w, t)^{-1} = (-u, -w, -t + \phi(u, w))$
- $[(u, w, t), (u', w', t')] = \phi(u, w') - \phi(u', w) \in T$

Groups and algebras

- T is central in G resp. in $\mathfrak{g}$
- G resp. $\mathfrak{g}$ is nilpotent of class at most 2
  [Elements of $[\mathrm{G}, \mathrm{G}]$ resp. $[\mathfrak{g}, \mathfrak{g}]$ are central]
- G and $\mathfrak{g}$ are related via famous correspondences
  Lazard's correspondence, Baer's correspondence, ...

Remark. Setting $\det \mathrm{B}(\mathbf{y}) = 0$ defines an affine variety $\mathcal{V}_{\mathrm{B}} \subseteq \mathbb{A}_k^d$. Moreover, since $\det \mathrm{B}(\mathbf{y})$ is a homogeneous polynomial, we have also a projective variety $\mathbb{P}\mathcal{V}_{\mathrm{B}} \subseteq \mathbb{P}_k^{d-1}$ associated to $\det \mathrm{B}(\mathbf{y})$.

Example. (du Sautoy, Vaughan-Lee, 2012) The matrix

$$\mathrm{B}_* = \begin{pmatrix} y_3 & -y_2 & y_1 \\ -y_2 & -y_1 & 0 \\ y_1 & 0 & y_3 \end{pmatrix}$$

satisfies $\det \mathrm{B}_* = y_1^3 - y_1 y_3^2 - y_2^2 y_3$, defining the elliptic curve

$$E_* : \quad y^2 = x^3 - x \text{ over } \mathbb{Q}.$$

For each odd prime p, the group $\mathbf{G}_{\mathrm{B}_*}(\mathbb{F}_p)$ has order p^9, class 2, and exponent p.

Theorem (du Sautoy, Vaughan-Lee, 2012)

The following function $\Pi \to \mathbb{Z}_{\geq 0}$ *is not PORC:*

$$p \mapsto \#\{\text{imm. desc. of } \mathbf{G}_{\mathrm{B}_*}(\mathbb{F}_p) \text{ of exponent } p \text{ and order } p^{10}\}/\cong$$

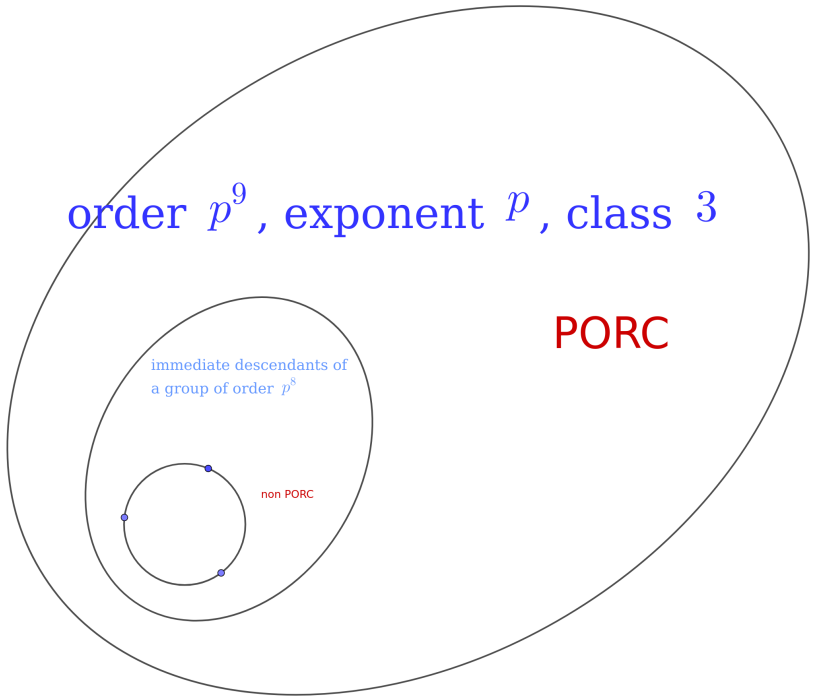
This strongly depends on $p \mapsto |\operatorname{Aut}(\mathbf{G}_{\mathrm{B}_*}(\mathbb{F}_p))|$ not being PORC.

$$\frac{|\operatorname{Aut}(\mathbf{G}_{\mathrm{B}_*}(\mathbb{F}_p))|}{p^{18}|\operatorname{GL}_2(\mathbb{F}_p)|} = \begin{cases} 4 & \text{if } p \equiv 1 \bmod 12 \text{ and } |E_*[3](\mathbb{F}_p)| = 1, \\ 36 & \text{if } p \equiv 1 \bmod 12 \text{ and } |E_*[3](\mathbb{F}_p)| \neq 1, \\ 6 & \text{if } p \equiv -1 \bmod 12, \\ 4 & \text{if } p \equiv 5 \bmod 12, \\ 2 & \text{if } p \equiv 7 \bmod 12. \end{cases}$$

The last theorem was proposed as a possible obstruction to PORC being true for $n = 10$. However,

"the local non-PORC behaviour of the counting functions does not necessarily imply non-PORCness on a larger domain"

More examples by: Lee (2016) and Vaughan-Lee (2018).



PROOF OF THE MAIN THEOREM

Symmetric determinantal representations and a family of curves

Theorem (S-Voll, 2020+)

Let E be an elliptic curve over $\mathbb{Q}$ and let K be a finite field of odd characteristic p over which E has good reduction. Assume, moreover, that $|E[2](K)| = 4$. Then there exist groups $\mathbf{G}_1(K)$, $\mathbf{G}_2(K)$, and $\mathbf{G}_3(K)$ satisfying:

- *for each $i = 1, 2, 3$, there exists $T_i \leq E \rtimes \mathrm{Aut}(E)$ such that*

$$|\operatorname{Aut} \mathbf{G}_i(K)| = |K|^{18} \cdot |\operatorname{GL}_2(K)| \cdot |T_i(K)| \cdot |\operatorname{Gal}(K/\mathbb{F}_p)|;$$

- *if $\delta \in \mathbb{Z} \setminus \{0\}$ and E is given by $y^2 = x^3 - x/\delta$, then*

$$T_i = E[3] \rtimes \mathrm{Aut}(E)[\lceil 4/i \rceil];$$

- *any two δ's modulo p yield 4 or 6 pairwise non-isomorphic groups of order $|K|^9$, exponent p, and nilpotency class 2.*

Theorem (Hesse, 1844)

Let $F \in \overline{k}[x,y,z]$ homogeneous be such that $F = 0$ defines an elliptic curve E. Then there are, up to equivalence, exactly three symmetric linear determinantal representations of E corresponding to the three solutions $(\alpha, \beta) \in \overline{k}^2$ of $\alpha F = \mathrm{Hes}(\beta F + \mathrm{Hes}(F))$.

Here: $B \sim B' \Leftrightarrow \exists U \in \mathrm{GL}_3(\overline{k})$ s.t. $B' = UBU^{\mathrm{t}}$

Remark. If E is defined over K, then the equivalence classes of symmetric determinantal representations of E are in one-to-one correspondence with the non-trivial 2-torsion points over K.

Remark. This yields the existence of $\mathbf{G}_1(K)$, $\mathbf{G}_2(K)$, $\mathbf{G}_3(K)$ and related algebras.

Recall that, B and ϕ are related via choices of bases: with respect to those we can view $\mathrm{Aut}(\mathfrak{g}) = \mathrm{Aut}_K(\mathfrak{g})$ as a subgroup of $\mathrm{GL}_{3d}(K)$ where each element is of the form

$$\alpha = \begin{pmatrix} A_U & A_{WU} & 0 \\ A_{UW} & A_W & 0 \\ C & D & A_T \end{pmatrix}$$

For $V = U \oplus W$, the group $\mathrm{Aut}(\mathfrak{g})$ has some natural subgroups

$$\mathrm{Aut}_V(\mathfrak{g}) = \{\alpha \in \mathrm{Aut}(\mathfrak{g}) \mid \alpha(V) = V\} \rightsquigarrow C = D = 0$$

$$\downarrow$$

$$\mathrm{Aut}_V^{\mathrm{f}}(\mathfrak{g}) = \{\alpha \in \mathrm{Aut}_V(\mathfrak{g}) \mid \alpha(U) = U,\ \alpha(W) = W\} \rightsquigarrow \text{and also } A_{UW} = A_{WU} = 0$$

$$\downarrow$$

$$\mathrm{Aut}_V^{=}(\mathfrak{g}) \rightsquigarrow \text{and also } A_U = A_W$$

The bullet dual of B is

$$\mathrm{B}^{\bullet} = \mathrm{B}^{\bullet}(\mathbf{x}) = \Big(\sum_{j=1}^{d} \mathrm{B}_{ij}^{(k)} \, x_j \Big)_{i,k=1}^{d}.$$

Other characterization: $\phi(u, w) = w \, \mathrm{B}^{\bullet}(u) \, (= \mathrm{ad}_u(w))$.

Example.

$$(1) \;\; \mathrm{B}(\mathbf{y}) = \begin{pmatrix} y_1 + y_2 & -y_1 \\ -y_1 & 0 \end{pmatrix} \;\Rightarrow\; \mathrm{B}^{\bullet}(\mathbf{x}) = \begin{pmatrix} x_1 - x_2 & x_1 \\ -x_1 & 0 \end{pmatrix}$$

(2) If B is Hessian, i.e. there exists $f(\mathbf{y}) \in R[y_1, \ldots, y_d]$ with

$$\mathrm{B}(\mathbf{y}) = \mathrm{H}(f(\mathbf{y})) = (\partial f(\mathbf{y}) / (\partial y_i \partial y_j))_{i,j=1}^{d},$$

then $\mathrm{B}(\mathbf{y}) = \mathrm{B}^{\bullet}(\mathbf{y})$.

Now $d = 3$, $\mathrm{B} = \mathrm{B}^\bullet$ is symmetric, and $\mathbb{P}\mathcal{V}_\mathrm{B} = E$. Recall

$$\alpha = \begin{pmatrix} A_U & A_{WU} & 0 \\ A_{UW} & A_W & 0 \\ C & D & A_T \end{pmatrix}$$

- $\mathrm{Aut}(\mathfrak{g}) \cong K^{2d^2} \rtimes \mathrm{Aut}_V(\mathfrak{g})$
- define $\psi(\mathrm{GL}_2(K))$ to be the collection of all

$$\alpha = \begin{pmatrix} a\,\mathrm{I}_3 & b\,\mathrm{I}_3 & 0 \\ c\,\mathrm{I}_3 & d\,\mathrm{I}_3 & 0 \\ 0 & 0 & (ad-bc)\,\mathrm{I}_3 \end{pmatrix} \text{ for } ad - bc \neq 0.$$

  Then $\mathrm{Aut}_V(\mathfrak{g}) = \psi(\mathrm{GL}_2(K))\,\mathrm{Aut}_V^f(\mathfrak{g})$ with intersection isomorphic to $K^* \times K^*$.
- $\mathrm{Aut}_V^f(\mathfrak{g}) \cong K^* \rtimes \mathrm{Aut}_V^=(\mathfrak{g})$.

For K finite:

$$|\mathrm{Aut}(\mathfrak{g})| = |K|^{18}|\mathrm{Aut}_V(\mathfrak{g})| = \frac{|K|^{18}|\mathrm{GL}_2(K)| \cdot |\mathrm{Aut}_V^=(\mathfrak{g})|}{|K^*|}$$

Lemma. For each $u \in U$, one has

$$\dim_K \mathrm{C}_V(u) = \begin{cases} 6, & \text{if } u = 0, \\ 4, & \text{if } u \in \mathcal{V}_{\mathrm{B}\bullet}(U) \setminus \{0\}, \\ 3, & \text{otherwise.} \end{cases}$$

This yields a well-defined homomorphism of groups

$$\varphi : \mathrm{Aut}^{=}_{V}(\mathfrak{g}) \to E(K) \rtimes \mathrm{Aut}(E)(K)$$

with kernel isomorphic to K^*.

Example. If E is given by $y^2 = x^3 - x/\delta$, then

$$\mathrm{Im}\,\varphi = \begin{cases} E[3](K) \rtimes \mathrm{Aut}(E)(K) & \text{if } \mathrm{B} \leftrightarrow (0,0), \\ E[3](K) \rtimes \mathrm{Aut}(E)[2](K) & \text{otherwise.} \end{cases}$$

Going back to the groups:

$$\begin{aligned} |\operatorname{Aut}(\mathrm{G})| &= |\operatorname{Aut}(\mathfrak{g})| \cdot |\operatorname{Gal}(K/\mathbb{F}_p)| \\ &= |K|^{18} \cdot |\operatorname{GL}_2(K)| \cdot |\operatorname{Im}\varphi| \cdot |\operatorname{Gal}(K/\mathbb{F}_p)| \end{aligned}$$

Regarding the isomorphism between groups...

Going back to the groups:

$$\begin{aligned} |\operatorname{Aut}(\mathrm{G})| &= |\operatorname{Aut}(\mathfrak{g})| \cdot |\operatorname{Gal}(K/\mathbb{F}_p)| \\ &= |K|^{18} \cdot |\operatorname{GL}_2(K)| \cdot |\operatorname{Im}\varphi| \cdot |\operatorname{Gal}(K/\mathbb{F}_p)| \end{aligned}$$

Regarding the isomorphism between groups...

Some open questions:

- A formula for all elliptic curves?
- A formula for non-symmetric representations?
- A general theory for groups coming from determinantal varieties?


thank you