LOCAL CYCLICITY OF ISOGENY CLASSES OF ABELIAN VARIETIES
DEFINED OVER FINITE FIELDS

ALEJANDRO J. GIANGRECO-MAIDANA

Abstract. For a prime number ℓ, an isogeny class A of abelian varieties is called ℓ-cyclic if every variety in A have a cyclic ℓ-part of its group of rational points. More generally, for a finite set of prime numbers S, A is said to be S-cyclic if it is ℓ-cyclic for every ℓ ∈ S. We give lower and upper bounds on the fraction of S-cyclic g-dimensional isogeny classes of abelian varieties defined over the finite field $\mathbb{F}_q$, when q tends to infinity.

1. Introduction

The group of rational points $A(k)$ of an abelian variety $A$ defined over a finite field $k = \mathbb{F}_q$ is a finite abelian group, and it has theoretical and practical interests. More precisely, the group structure of $A(k)$ and some statistics are research topics in the literature.

The structure of all possible groups for elliptic curves defined over finite fields was independently discovered in [8], [6], [10] and [13]. For higher dimensions, Rybakov gives in [7] a very explicit description of all possible groups of rational points of an abelian variety in a given isogeny class, his result is formulated in terms of the characteristic polynomial of the isogeny class.

Cyclic subgroups of the group of rational points $A(k)$ of an abelian variety $A$ defined over a finite field $k$ are suitable for multiple applications, in particular for cryptography, where the Discrete Logarithm Problem is exploited. Elliptic curves with cyclic groups of rational points are of special interest, and many algorithms chooses it randomly. Thus, knowing such statistics can be useful. Statistics on the fraction of isomorphism classes of elliptic curves that are cyclic were explored in [11] and [12], and for higher dimensions, this was explored in [2].

More precisely, in [2] we studied the cyclicity of isogeny classes of abelian varieties defined over finite fields. In particular, if $S$ is a finite set of prime numbers, from these results we can easily deduce a nice criterion to know if an isogeny class $A$ is $S$-cyclic, i.e., for every variety $A \in A$ and every $\ell \in S$, the $\ell$-part $A(k)_{\ell}$ of $A(k)$ is cyclic. This criterion is based on the characteristic polynomial of the isogeny class $A$. Clearly, this result is meaningful only if $A(k)_{\ell}$ is nontrivial.

As a consequence of Tate theorem ([9]), the cardinality of $A(k)$ is an invariant of the isogeny class, and thus, the property of $A(k)_{\ell}$ to be or not trivial is an invariant of the isogeny class as well.

Using the strategy proposed in [1], Holden proved in [3] that the fraction of k-isogeny classes with nontrivial $\ell$-part $A(k)_{\ell}$ is asymptotically $1/\ell$, when q tends to infinity.

1991 Mathematics Subject Classification. Primary 11G10, 14G15, 14K15.
Key words and phrases. group of rational points, cyclic, local, abelian variety, finite field.
In this paper, we combine both results (from [2] and [3]) to provide lower and upper (asymptotic) bounds, in Theorem 2.1, on the fraction of \( k \)-isogeny classes of abelian varieties that are \( S \)-cyclic, among those \( k \)-isogeny classes with a nontrivial \( \ell \)-part, for at least one \( \ell \in S \).

The rest of this paper is organized as follows: in Section 2 we briefly recall some general facts about abelian varieties over finite fields and we state our result more precisely; in Section 3 we prove Theorem 2.1; finally, in Section 4 (Appendix) we prove some propositions used in the proof of Theorem 2.1.

2. Preliminaries and Statement of the results

Let establish the results more precisely. From the Honda-Tate theorem ([9, 4]), every isogeny class \( A \) of abelian varieties defined over a finite field is uniquely determined by its Weil polynomial \( f_A(t) \in \mathbb{Z}[t] \), the characteristic polynomial of its Frobenius endomorphism acting on its Tate module. The cardinality of the group of rational points of a variety \( A \) in \( A \) equals \( f_A(1) \), thus is an invariant of the isogeny class. Let \( q = p^r \) be a power of a prime and denote by \( I(q, g) \) the set of \( g \)-dimensional isogeny classes \( A \) of abelian varieties defined over the finite field \( \mathbb{F}_q \).

For a fixed and finite set of prime numbers \( S \) (even containing \( p \)), we say that an isogeny class \( A \) is \( S \)-cyclic if all its varieties have a cyclic \( \ell \)-part of its group of rational points for all \( \ell \in S \).

For more details on the general theory of abelian varieties see for example [5], and for precise results over finite fields, see [14].

Following the notation in [3], we define the following cardinalities

- \( I_S(q, g) = \# \{ A \in I(q, g) : \ell | f_A(1) \text{ for some prime } \ell \in S \} \) (those with \( (A(k))_\ell \) non trivial)
- \( I^n_S(q, g) = \# \{ A \in I(q, g) : \ell | f_A(1) \text{ with } A \text{ non } S\text{-cyclic } \} \).

Then, our result provides the proportion of \( S \)-cyclic isogeny classes:

**Theorem 2.1.** There exist a \( q_0 = q_0(S) \), such that if \( q \geq q_0 \), we have

\[
1 - \frac{1 - \sigma_2(S)}{1 - \sigma_1(S)} \leq \frac{I_S(q, g) - I^n_S(q, g)}{I_S(q, g)} \leq 1 - \frac{1 - \sigma_3(S)}{1 - \sigma_1(S)},
\]

where

\[
\sigma_1(S) = \prod_{\ell \in S} \left(1 - \frac{1}{\ell^n}\right).
\]

**Remarks 2.2.**

1. If we consider the sets \( S(N) = \{ \ell \text{ prime} : \ell \leq N \} \), then when \( N \to \infty \), \( \sigma_i(S(N)) \to 1/\zeta(i) \), where \( \zeta \) is the Riemann zeta function. Thus, since \( \zeta(1) = \infty \), the bounds can be simplified

\[
0.6 \approx \frac{1}{\zeta(2)} \leq \frac{I_{S(N)}(q, g) - I^n_{S(N)}(q, g)}{I_{S(N)}(q, g)} \leq \frac{1}{\zeta(3)} \approx 0.833.
\]

Computational results show that these limits start in 0.5 and 0.75 (when \( N = 2 \)) and establish quickly at 0.57 and 0.815 (around \( N = 557 \)).
and for simplicity, we write it as $f$ class, and we will clarify it in the next paragraph. For a polynomial of the previous form $f$, we associate another polynomial $R$.

$$f^{(2)}(t) = \frac{1}{2} \left( \frac{q}{\ell} \right), \text{ when } q \text{ tends to infinity among such } q \text{ with } \ell | (q-1) \text{ or } \ell \not| (q-1), \text{ respectively.}$$

Considering the result in [3], this means that the fraction of isogeny classes with non-trivial $\ell$-part is approximately $\frac{1}{\ell}$.

(3) From [3] we can see that the fraction of isogeny classes with non-trivial $\ell$-part for at least one $\ell \in S$ is $1 - \sigma_1(S)$.

3. The proof

Here we prove Theorem 2.1. Also, for the clarity of the text, the propositions used for the proofs of theorems are proved in the Appendix.

Our procedure is based on the method of counting isogeny classes of abelian varieties introduced by DiPippo and Howe [1], after having done some partitions in particular lattices, similar as in [3].

We will consider rectilinear lattices, by which we mean lattices that have a rectilinear fundamental domain with edges parallel to the coordinate axes. The covolume of a lattice $\Lambda$ is the volume of a fundamental domain $R$ of $\Lambda$, and the mesh of $\Lambda$ is the length of the longest edge of $R$.

Every isogeny class $\mathcal{A}$ is defined by its Weil polynomial $f_{\mathcal{A}}$, which has the general form

$$f_{\mathcal{A}}(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + a_{g-1} q t^{g-1} + \cdots + a_1 q^{g-1} t + q^g \in \mathbb{Z}[t],$$

and for simplicity, we write it as $f_{\mathcal{A}}(a_1, \ldots, a_g)(t)$. Not every polynomial of the previous form defines an isogeny class, but we know “almost all” polynomials that are Weil polynomials of some isogeny class, and we will clarify it in the next paragraph. For a polynomial of the previous form $f_{\mathcal{A}}(t)$, we associate another polynomial

$$h_b(t) = f_{\mathcal{A}}(b) / q^g = (t^{2g} + 1) + b_1 (t^{2g-1} + t) + \cdots + b_{g-1} (t^{g+1} + t^{2g-1}) + b_g t^g \in \mathbb{R}[t].$$

We consider three types of lattices. The first one, $\Lambda_q$, is generated by the vectors $q^{-i/2} e_i$, where $e_1, \ldots, e_g$ denote the standard basis vectors of $\mathbb{R}^g$. From DiPippo and Howe [1], it follows that if an isogeny class has $f_{\mathcal{A}}(t)$ as its Weil polynomial, then $(a_1 q^{-1/2}, \ldots, a_g q^{-g/2}) \in \Lambda_q \cap V_g$, where $V_g$ is the set of vectors $b = (b_1, \ldots, b_g) \in \mathbb{R}^g$ such that the associated $h_b(t)$ has all its roots on the unit circle and all its real roots occur with multiplicity. The second lattice, $\Lambda'_q$, is generated by the vectors $q^{-i/2} e_1, \ldots, q^{-(g-1)/2} e_{g-1}$ and $pq^{-g/2} e_g$. Then, there is a bijection between isogeny classes of ordinary varieties with Weil polynomial $f_{\mathcal{A}}(t)$, and $(\Lambda_q \setminus \Lambda'_q) \cap V_g$, given by $a \mapsto (a_1 q^{-1/2}, \ldots, a_g q^{-(g-1)/2})$. Finally, the third lattice, $\Lambda''_q$, is generated by the vectors $q^{-i/2} e_1, \ldots, q^{-(g-1)/2} e_{g-1}$ and $sq^{-g/2} e_g$, where $s$ is the smallest power of $p$ such that $q$ divides $s^2$. Then every non-ordinary isogeny class has its Weil polynomial $f_{\mathcal{A}}(t)$ such that $(a_1 q^{-1/2}, \ldots, a_g q^{-(g-1)/2}) \in \Lambda''_q \cap V_g$. In order to measure the sizes of these kind of sets (we will refine these lattices later), we will use Proposition 2.3.1 of [1] in a generalized form:
Proposition 3.3. Let \( \Lambda \subset \mathbb{R}^g \) be a rectilinear lattice (possibly shifted) with mesh \( d \) at most \( D \). Then we have

\[
\frac{\#(\Lambda \cap V_g) - \text{volume}\frac{V_g}{\text{covolume}\Lambda}}{d} \leq c(g, D)
\]

for some constant \( c(g, D) \) depending only on \( g \) and \( D \) which can be explicitly computed. (We will not need the explicit computation in this paper.)

Denote by \( F = F(S) \) the product of primes contained in \( S \). From Theorem 2.2 in [2], we have that \( \mathcal{A} \) is not cyclic if and only if \( (f(1), f'(1)) > 1 \), where \( \hat{z} \) is the integer \( z \) divided by the product of its different prime divisors. Locally, \( \mathcal{A} \) is not \( \ell \)-cyclic if and only if \( \ell |(f(1), f'(1)) \).

Then, we have a partition of the form

\[
I_S(q, g) = \sum I_m(q, g),
\]

\[
I_S^2(q, g) = \sum I_m(q, g),
\]

where the summations on equations (3) and (4) are taken, respectively, over

- all \( m \in (\mathbb{Z}/F^2\mathbb{Z})^g \), such that \( f_{q, m}(1) \) is not invertible in \( \mathbb{Z}/F^2\mathbb{Z} \), i.e., such that \( A(\mathbb{F}_q) \ell \) is not trivial for some \( \ell \in S \), and
- all \( m \in (\mathbb{Z}/F^2\mathbb{Z})^g \), such that \( \ell |(f(1), f'(1)) \) for some \( \ell \in S \), i.e., \( A(\mathbb{F}_q) \) have some non-cyclic component;

and where \( I_m(q, g) \) is the number of isogeny classes of \( g \)-dimensional abelian varieties over \( \mathbb{F}_q \) with Weil polynomial \( f_{q, m} \) for some \( a \in \mathbb{Z}^g \) such that \( a \equiv m \pmod{F^2} \). The number of terms on the right side of equations above will be important, and we will see it in a proposition below.

Now we refine the lattices mentioned above, and we will calculate their sizes using Proposition 3.1. If \( \Lambda_m \) is the lattice generated by the vectors \( F^2q^{-i/2}e_i \) and then shifted by \( \sum m_iq^{-i/2}e_i \), we consider the lattices \( \Lambda'_m = \Lambda_m \cap \Lambda'_q \) and \( \Lambda''_m = \Lambda_m \cap \Lambda''_q \). Set \( G = g(g + 1)/4 \), then \( \Lambda_m \) has covolume \( F^{2g}q^{-G} \) and mesh \( F^2q^{-1/2} \); \( \Lambda'_m \) has covolume \( F^{2g}pq^{-G} \) and mesh \( F^2q^{-1/2} \) unless \( g = 2 \) and \( q = p \) in which case it has mesh \( F^2 \); and \( \Lambda''_m \) has covolume \( F^{2g}sq^{-G} \) and mesh at most \( F^2 \).

From Proposition 3.1 we get (see Appendix for the proof)

Proposition 3.2.

\[
L(q, g, F)F^{-2g} \leq I_m(q, g) \leq R(q, g, F)F^{-2g},
\]

with

\[
L(q, g, F) = \left(v_g r(q)q^G - 2F^2c(g, F^2)q^{G-1/2}\right)
\]

and

\[
R(q, g, F) = \left(v_g r(q)q^G + (v_g + 3F^2c(g, F^2))q^{G-1/2}\right),
\]

and where \( v_g \) is the volume of \( V_g \) and \( r(q) = 1 - 1/p \).

Note that \( L/R \) tends to 1 when \( q \) tends to infinity. Also, we can show that (see Appendix for the proof)

Proposition 3.3.
Thus, from the description of DiPippo and Howe,

Thus we get

\[ (1 - \sigma_1(S))L(q, g, F) \leq IS(q, g) \leq (1 - \sigma_1(S))R(q, g, F), \]

\[ (1 - \sigma_3(S))L(q, g, F) \leq IS(q, g) \leq (1 - \sigma_2(S))R(q, g, F), \]

then, when \( q \) tends to infinity

\[ \frac{1 - \sigma_3(S)}{1 - \sigma_1(S)} \leq \frac{IS(q, g)}{I_S(q, g)} \leq \frac{1 - \sigma_2(S)}{1 - \sigma_1(S)} \]

which gives the result. Theorem 2.1 is thus proved.

4. APPENDIX

Proof of Proposition 3.2 Here we prove the \( S \)-case. For simplicity, we omit the subscript \( m \) from \( I_m(q, g), \Lambda_m, \Lambda'_m \) and \( \Lambda''_m \), and we write \( v \) instead of \( v_g \). Concerning these three lattices, we summarize its values in the following table

| \( \Lambda \) | \( F^{2g}q^{-G} \) | \( F^{2}q^{-1/2} \) | \( d \) | \( D \) | \( d/covolume \) |
|---|---|---|---|---|---|
| \( \Lambda \) | \( F^{2g}q^{-G} \) | \( F^{2}q^{-1/2} \) | \( d \) | \( D \) | \( d/covolume \) |
| \( \Lambda' \) | \( F^{2q}pq^{-G} \) | \( F^{2}q^{-1/2} \) | \( F^{2}q^{-2g}q^{G-1/2}/p \) | \( F^{2}q^{-1/2} \) | \( F^{2}q^{G}/s \) |
| \( \Lambda'' \) | \( F^{2q}sq^{-G} \) | \( F^{2}q^{G}/s \) | \( F^{2}q^{-2g}q^{G-1/2}/p \) | \( F^{2}q^{-1/2} \) | \( F^{2}q^{G}/s \) |

We apply Proposition 3.1 which in the general form says

\[
\frac{\text{volume } V_g}{\text{covolume } \Lambda} - c(g, D) \frac{d}{\text{covolume } \Lambda} \leq \#(\Lambda \cap V_g) \leq \frac{\text{volume } V_g}{\text{covolume } \Lambda} + c(g, D) \frac{d}{\text{covolume } \Lambda},
\]

thus, for every lattice we get, respectively

\[
vF^{-2g}q^{G} - c(g, F^2)F^{2-2g}q^{G-1/2} \leq \#(\Lambda \cap V_g) \leq vF^{-2g}q^{G} + c(g, F^2)F^{2-2g}q^{G-1/2}
\]

\[
vF^{-2g}q^{G}/p - c(g, F^2)F^{2-2g}q^{G-1/2}/p \leq \#(\Lambda' \cap V_g) \leq vF^{-2g}q^{G}/p + c(g, F^2)F^{2-2g}q^{G-1/2}/p
\]

\[
vF^{-2g}q^{G}/s - c(g, F^2)F^{2-2g}q^{G-1/2}/s \leq \#(\Lambda'' \cap V_g) \leq vF^{-2g}q^{G}/s + c(g, F^2)F^{2-2g}q^{G-1/2}/s
\]

From the description of DiPippo and Howe,

\[
\#((\Lambda' \setminus \Lambda') \cap V_g) \leq I(q, g) \leq \#((\Lambda' \cup \Lambda'' \setminus \Lambda') \cap V_g)
\]

Thus,

\[
I(q, g) \geq vF^{-2g}q^{G} - c(g, F^2)F^{2-2g}q^{G-1/2} - \left( vF^{-2g}q^{G}/p + c(g, F^2)F^{2-2g}q^{G-1/2}/p \right)
\]

\[
= vF^{-2g}q^{G}r(q) - c(g, F^2)F^{2-2g}q^{G-1/2}(1 + 1/p)
\]

\[
\geq vF^{-2g}q^{G}r(q) - 2c(g, F^2)F^{2-2g}q^{G-1/2}.
\]
Also (knowing that $s$ is roughly $\sqrt{q}$ and $\sqrt{q} \leq s$),

$$I(q, g) \leq vF^{-2g}q^G + c(g, F^2)F^{2-2g}q^{G-1/2} - \left(vF^{-2g}q^G/p - c(g, F^2)F^{2-2g}q^{G-1/2}/p\right) + vF^{-2g}q^G/s + c(g, F^2)F^{2-2g}q^G/s$$

$$= vF^{-2g}r(q)q^G + vF^{-2g}q^{G-1/2} + c(g, F^2)F^{2-2g} \left(q^{G-1/2}/p + q^G/s\right)$$

$$\leq vF^{-2g}r(q)q^G + vF^{-2g}q^{G-1/2} + c(g, F^2)F^{2-2g} \left(q^{G-1/2}/p + q^{G-1/2}\right)$$

$$= vF^{-2g}r(q)q^G + (v + 3F^2c(g, F^2))F^{-2g}q^{G-1/2}$$

Thus, the proposition is proved. 

**Proof of the Proposition 3.3.** Knowing the number of terms of these equations is equivalent to knowing the number of solutions of certain systems of equations.

The first item follows from the fact that the number of solutions is $F^{2g-2}(\varphi(F^2))$, where $\varphi$ is the Euler’s totient function, since for every $n \in (\mathbb{Z}/F^2\mathbb{Z})^g-1$, there are exactly $F^2 - \varphi(F^2)$ of $x$ satisfying that $f_q(n,x,1)$ is not invertible in $\mathbb{Z}/F^2\mathbb{Z}$.

For the second item, it means, there exist a prime $\ell \in S$ such that

$$f_q(1) \equiv i\ell^2 \pmod{F}$$

$$f'_q(1) \equiv j\ell \pmod{F}$$

We can study locally by the well known isomorphism

$$(\mathbb{Z}/F^2\mathbb{Z})^g \cong \prod_{\ell \mid F} \left(\mathbb{Z}/\ell^2\mathbb{Z}\right)^g$$

In this case, the number of solution is between $\ell^{2g-3}$ and $\ell^{2g-2}$ (see below for the proof). Then the result follows from the inclusion-exclusion formula, since we have a solution of the problem if and only if we have a solution on at least one component. Now, we study the problem locally, and we split it in two cases:

When $\ell \nmid q - 1$, for every $n \in (\mathbb{Z}/\ell^2\mathbb{Z})^{g-2}$, the system

$$f_q(n,x,y)(1) \equiv 0 \pmod{\ell^2}$$

$$f'_q(n,x,y)(1) \equiv i\ell \pmod{\ell^2}, i = 0, 1, \ldots, \ell - 1$$

has exactly $\ell$ solutions (exactly one for every $i$ on the second equation), since we can write

$$f_q(n,x,y)(1) = h_1(n) + (q + 1)x + y$$

and

$$f'_q(n,x,y)(1) = h_2(n) + [g(q + 1) + 1 - q]x + gy$$

which determinant is $q - 1 \pmod{\ell^2}$.

When $\ell \mid q - 1$, we have

$$f_q(a)(1) \equiv 2 + 2a_1 + \cdots + 2a_{g-1} + a_g \pmod{\ell}$$

$$f'_q(a)(1) \equiv g(2 + 2a_1 + \cdots + 2a_{g-1} + a_g) \equiv gf_q(a)(1) \pmod{\ell}$$

i.e., $f' \equiv gf \pmod{\ell}$, which means $f' - gf \equiv i\ell \pmod{\ell^2}$ for some $i$, thus, if $a$ is a solution for the first equation, $f' \equiv i\ell \pmod{\ell^2}$, which means $f' \equiv 0 \pmod{\ell}$. Now, for every $n \in (\mathbb{Z}/\ell^2\mathbb{Z})^{g-1}$,
we have exactly one solution for the first equation, and which is automatically a solution for the second equation by the previous explanation. Thus, the result follows.

Acknowledgement

I would like to thank my advisor Serge Vlăduț for very fruitful discussions and for his very useful comments and suggestions.

References

[1] S. A. DiPippo and E. W. Howe, Real polynomials with all roots on the unit circle and abelian varieties over finite fields, Journal of Number Theory, 73 (1998), pp. 426 – 450.
[2] A. J. Giangreco-Maidana, On the cyclicity of the rational points group of abelian varieties over finite fields, arXiv preprint arXiv:1806.10842, (2018).
[3] J. Holden, Abelian varieties over finite fields with a specified characteristic polynomial modulo ℓ, Journal de Théorie des Nombres de Bordeaux, 16 (2004), pp. 173–178.
[4] T. Honda, Isogeny classes of abelian varieties over finite fields, J. Math. Soc. Japan, 20 (1968), pp. 83–95.
[5] D. Mumford, Abelian varieties, vol. 5 of Tata Institute of fundamental research studies in mathematics, Oxford University Press, 1970.
[6] H.-G. Rück, A note on elliptic curves over finite fields, Mathematics of Computation, 49 (1987), pp. 301–304.
[7] S. Rybakov, The groups of points on abelian varieties over finite fields, Central European Journal of Mathematics, 8 (2010), pp. 282–288.
[8] R. Schoof, Nonsingular plane cubic curves over finite fields, Journal of Combinatorial Theory, Series A, 46 (1987), pp. 183 – 211.
[9] J. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math., 2 (1966), pp. 134–144.
[10] M. A. Tsfasman, Group of points of an elliptic curve over a finite field, Theory of numbers and its applications, Tbilisi, (1985), pp. 286–287.
[11] S. G. Vlăduț, Cyclicity statistics for elliptic curves over finite fields, Finite Fields and Their Applications, 5 (1999), pp. 13 – 25.
[12] ———, On the cyclicity of elliptic curves over finite field extensions, Finite Fields and Their Applications, 5 (1999), pp. 354 – 363.
[13] J. F. Voloch, A note on elliptic curves over finite fields, Bull. Soc. Math. France, 116 (1988), pp. 455–458.
[14] W. C. Waterhouse, Abelian varieties over finite fields, Annales scientifiques de l’École Normale Supérieure, 2 (1969), pp. 521–560.

Aix Marseille Université, CNRS, Centrale Marseille, I2M UMR 7373, 13453 Marseille, France
E-mail address: ajgiangreco@gmail.com