On arithmetic properties of abelian varieties over finite fields.

Pavel Solomatin

05.2012

Abstract

In this paper, we are going to discuss some arithmetic properties of abelian varieties over finite fields. An interesting question is to find out how many points there can be on a curve or abelian variety over a finite field. To each isogeny class of abelian varieties X over $\mathbb{F}_q$ one can associate the Weil polynomial f_X. Here we study the behaviour of the volume of the set of Weil polynomials of a given degree with certain restrictions on their roots which correspond to the bounds for the number of points on curves in the case of the Jacobians over finite fields. We also study a similar question about points on abelian varieties.

1 The main goal and structure of the paper

The main purpose of this paper is to show one interesting approach to the study of the behaviour of the number of abelian varieties with many points over finite fields. This approach uses the parametrization of the Weil polynomials of abelian varieties.

Here we have $V_\alpha \subset \mathbb{R}^n$, $V_\alpha = \Phi(C_\alpha)$, where C_α is the convex polytope and Φ is the smooth map from $\mathbb{R}^n$ to $\mathbb{R}^n$, for complete definitions see section 2.3. By construction, the integer points in the set $\sqrt{q}V_\alpha = \{\sqrt{q}v \mid v \in V_\alpha\}$ correspond to the polynomials $f(x) \in \mathbb{Z}[x]$, with degree $2n$ such that:

1. all its complex roots x_i satisfy $|x_i| = \sqrt{q}$ and $f(0) = q^n$;
2. $\sum x_i \geq \alpha\sqrt{q}$.

On the other hand, such polynomials correspond to the isogeny classes of abelian varieties over $\mathbb{F}_q$. Namely, one and only one of the following statements is true:

1. $f(x)$ is Weil polynomials of isogeny class of abelian varieties A, such that $\dim(A) = n$. In this case, we have[1] $\frac{(q+1)^n - \#A}{(q+1)^{n-1}} \geq \alpha\sqrt{q}$. Define $M_{ord}(\alpha)$ by the set of all integer points $v \in \sqrt{q}V_\alpha$ such that $f_v(x)$ as above.

2. There is exists natural number $d > 1$, such $(f(x))^d$ is Weil polynomials for some isogeny class of abelian varieties. Define $M_{sin}(\alpha)$ by the set of all integer points $v \in \sqrt{q}V_\alpha$ such that $f_v(x)$ as above.

So, on the one hand we have:

$$\#\{\mathbb{Z}^n \cap \sqrt{q}V_\alpha\} = \#M_{ord}(\alpha) + \#M_{sin}(\alpha).$$

On the other hand, as $q \to \infty$ we obviously have that:

$$\#\{\mathbb{Z}^n \cap \sqrt{q}V_\alpha\} = q^{\frac{n}{2}}\,\mathrm{Vol}(V_\alpha) + \mathrm{O}\left(q^{\frac{n-1}{2}}\right).$$

Finally, here we study the proportion $P(\alpha) = \frac{\mathrm{Vol}(V_\alpha)}{\mathrm{Vol}(V_{-\infty})}$. Note that, as $q \to \infty$ we have:

$$\frac{\#\{\mathbb{Z}^n \cap \sqrt{q}V_\alpha\}}{\#\{\mathbb{Z}^n \cap \sqrt{q}V_{-\infty}\}} \to P(\alpha).$$

Also, we will use the function $P(\alpha)$ for the study the same question about the number of Jacobians with many points.

Note that:

$$\mathrm{Vol}(V_\alpha) = \int_{C_\alpha} \prod_{1 \leq j < i \leq n} (x_i - x_j)\; dx_1 \ldots\; dx_n.$$

Here we explicitly write out the above integral for $n = 1$, 2 and 3 and prove some statements about $P(\alpha)$. Also, we compare our results with well-known theorems about abelian varieties.

The paper has the following structure. In section 2 we describe the main statements about curves and abelian varieties. In section 3 we give the precise formulation of the main problems of this article. In the other section we study the main properties of $P(\alpha)$.

[1] for sufficiently large q.

2 Introduction

2.1 General setting

It is well known that in number theory elliptic curves and, more generally, abelian varieties, play an important role. There are several approaches to the study of properties of abelian varieties. The reduction to a finite field is one of them. This approach is good, because it makes some properties of abelian varieties more tractable. An example is a Riemann hypothesis still unsolved over $\mathbb{Q}$, but over finite fields this is a classical, though highly non-trivial, result. For more information or examples, one can look at [2] or [3].

Let us fix a finite field $k = \mathbb{F}_q$, where $q = p^n$ (p is prime) and consider a curve X over k. One of the interesting problems is to understand how many points there are on X over k.

Let $\#X(k)$ denote the number of points on curve X over filed k. There are many theorems that concern the number $\#X(k)$. The following classical result is known under the name of Weil bound:

Theorem 1. $|\#X(k) - q - 1| \leq 2g\sqrt{q}$, *where g is the genus of the curve X.*

The problem of improving this bound is very difficult. Many well known mathematicians devoted considerable efforts to its study. One of the possible approaches uses the theory of abelian varieties by means of associating the Jacobian variety to a curve. Then the number of points on the curve can be recovered from the roots of the Weil polynomials of the Jacobian.

2.2 Weil Polynomials

To an abelian variety A over k one associate the Weil polynomial f_A; it is the characteristic polynomial f_A of the Frobenius endomorphism acting on the Tate module of A. The degree of f_A is twice the dimension of A. Such polynomials play an important role in the theory of curves over finite fields. Now, we formulate the main properties of Weil polynomials. For more details see [3].

Definition 1. Weil q-number is an algebraic integer ζ such that for each embedding ψ of $\mathbb{Q}(\zeta)$ into the complex numbers $|\psi(\zeta)| = q^{\frac{1}{2}}$.

The following theorems concern the roots of Weil polynomials:

Theorem 2 (Weil). *1. The polynomial f_A has integer coefficients.*

2. All complex roots of the Weil polynomial f_A are Weil numbers.

3. For any abelian variety A we have $f_A(0) = q^n$, where n is the dimension of A.

Theorem 3 (Honda—Tate). *1. The isogeny class of an abelian variety A is uniquely determined by its Weil polynomial.*

2. Every Weil number is a root of some Weil polynomial. Moreover, the dimension of the corresponding abelian variety can be explicitly found, using the classfield theory.

So, there is a connection between n-dimensional abelian varieties and polynomials $f \in \mathbb{Z}[x]$, such that $\deg(f) = 2n$, all its complex roots α_i satisfy the condition $|\alpha_i| = \sqrt{q}$ and $f(0) = q^n$. More precisely, by using the above theorems one can prove the following corollary:

Corollary 1. *Let $f(x) \in \mathbb{Z}[x]$ is defined as above. Then, there exists an abelian variety A and natural number d such that the Weil polynomial $f_A(x)$ is $(f(x))^d$.*

One can try to use the above theorems for the study of arithmetics properties of abelian varieties. This approach was used by E.Howe.

2.3 Howe's approach

Our approach is based on the idea suggested in the article [1]. In this section, we review the most important points of this article.

First of all, we fix a real polynomial with integer coefficients f with all its complex roots lying on the circle of radius $\sqrt{q}$, centered at the origin. Furthermore, we suppose that if f has real roots ($\sqrt{q}$ or $-\sqrt{q}$), then they occur with even multiplicity.

After the variable change $x \to x\sqrt{q}$, we have $f(x) = q^n \prod_{i=1}^{n}(x^2 - r_i x + 1)$, where $-2 \leq r_i \leq 2$.

Definition 2. Let $b \in \mathbb{R}^n$, $b = (b_1, \ldots, b_n)$. We denote by $g_b(x)$ the polynomial $g_b = (x^{2n} + 1) + b_1(x^{2n-1} + x) + \ldots + b_{n-1}(x^{n+1} + x^{n-1}) + b_n x^n$.

By using the symmetry relation, we see that there is some vector $b \in \mathbb{R}^n$ such that $f(x) = q^n g_b(x)$ for all x.

Definition 3. Define V_n to be the set of all vectors $b \in \mathbb{R}^n$, such that all the roots of g_b are on the unit circle and its real roots occur with even multiplicity.

Up to scaling, the Weil polynomials of abelian varieties correspond to integer points in V_n. One can ask, how to describe V_n explicitly, or at least how to calculate the volume of V_n. In the article, [1] one can find the answer to this question. As it turned out, there exists a diffeomorphism $F(x_1, \ldots, x_n)$ from the simplex C_n to V_n. Therefore we may calculate this volume as an integral of the $\det |dF|$ over C_n. On the other hand dF may be calculated explicitly. By using the above facts, Howe proved, for example, the following theorem:

Theorem 4.

$$\mathrm{Vol}(V_n) = \int_{C_n} \det(dF)\ dx_1 \ldots dx_n = \frac{2^n}{n!} \prod_{i=1}^{n} \left(\frac{2i}{2i-1} \right)^{n+1-i}.$$

Also, in the Howes article one can find an application of this formula to the problem of counting the isogeny classes.

3 The main problems

In this section, we are going to formulate our main problems. Generally speaking, the first task is related to the estimation of the number of curves with many points over some finite field k. The second interesting question is to estimate the number of isogeny classes of abelian varieties with many points over k.

3.1 The basic facts

As we have already said, if X is a curve, then one can associate to X the Jacobian variety $J = \mathrm{Jac}(X)$. $\mathrm{Jac}(X)$ is an abelian variety, as a group the Jacobian is $\mathrm{Pic}^0(X)$. The dimension of the Jacobian is the genus of the curve X. For example, if X is an elliptic curve, then $g = 1$ and $\mathrm{Jac}(X) = X$. For more details see [5].

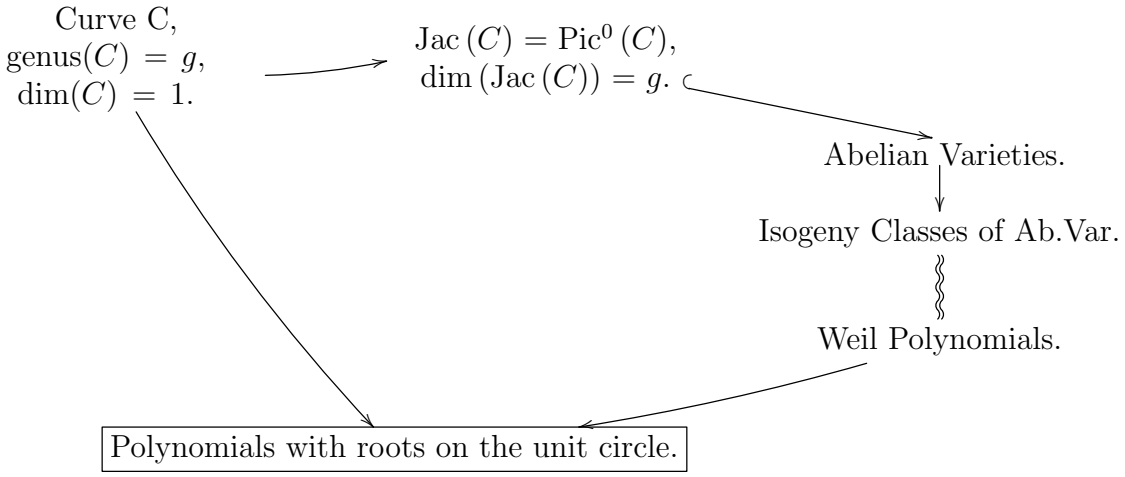
Les us consider $f_J(x)$, the Weil polynomial of $\mathrm{Jac}(X)$. Then one can prove the following theorems:

Theorem 5. *If* $f_J(x) = \prod (x - \alpha_i)$*, then* $\#X(k) = q + 1 - \sum \alpha_i$*.*

Theorem 6. *For any abelian variety* A *we have* $\#A(k) = f_A(1)$*.*

By using these facts we try to approximate the number of curves with large number of points over k. Namely, following Howe's idea, we ask how many Weil polynomials there are with large $\sum \alpha_i$. Similarly, we estimate the number of isogeny classes of abelian varieties with many points over k by previous counting the number of Weil polynomials f with large value $f(1)$. The question on the Weil polynomials is much rougher than the one about the curves, but we have to content ourselves with the solution of the former problem since the question on curves is too difficult at the moment.

The following diagram is very useful for understanding our approach:



Before we give the precise statements of this article, we have to describe the parametrization of V_n.

3.2 The parametrization of V_n

Here, we give an explicit description of the region V_n, see 1.3 for definition. Any polynomial f_b, where $b \in V_n$, can be written as $f_b = \prod_{i=1}^{n} (x^2 - r_i x + 1)$,

where $-2 \leq r_i \leq 2$. This is the key point for our construction.

Let C_n be the simplex $C_n = \{x \in \mathbb{R}^n | -2 \leq x_1 \leq \cdots \leq x_n \leq 2\}$ and let $r \in C_n$. Then we consider the polynomial $F(x) = \prod_{i=1}^{n}(x - r_i)$ and we define $f(x)$ as:

$$f(x) = x^n F\left(x + \frac{1}{x}\right) = x^n \prod_{i=1}^{n}\left(x + \frac{1}{x} - r_i\right) = \prod_{i=1}^{n}(x^2 - r_i x + 1).$$

We see that there is some $b \in V_n$, such that $f(x) = g_b(x)$.

Definition 4. Define the map $\Phi : C_n \to V_n$ as: $\Phi(r_1, \ldots, r_n) = (b_1, \ldots, b_k)$, where b_k is the k-th coefficient (or $(n-k)$-th because they are equal) of the polynomial $\prod_{i=1}^{n}(x^2 - r_i x + 1)$.

One can find an explicit formula for b_k using the elementary symmetric functions, but we just note that $b_1 = -\sum r_i$.

The following statements are almost obvious, for a complete proof see the Howe's article [1]:

Proposition 1. *The map Φ is a diffeomorphism. Moreover,*

$$\det(d\Phi) = \prod_{1 \leq j < i \leq n}(r_i - r_j).$$

4 On the number of curves with many points

Fix $\alpha \in \mathbb{R}$ and define $C_{n,\alpha} = \{x \in C_n | \sum x_i \geq \alpha\}$. Consider the set $V_{n,\alpha}$, which is the set of all vectors $b \in V_n$ such that: $b_1 \geq \alpha$. By using the remarks from the previous section one concludes that the map Φ is a diffeomorphism from $C_{n,\alpha}$ to $V_{n,\alpha}$.

Now note that the integer points in $V_{n,\alpha}$ contain the points corresponding to the isogeny classes of Jacobians of curves X such that:

$$(q+1) - \#X(\mathbb{F}_q) \geq \alpha\sqrt{q}.$$

Note also that, as q tends to infinity, the number of integer points in $V_{n,\alpha}$ tends to the volume of $V_{n,\alpha}$.

Definition 5. Define $P_n(\alpha) = \frac{\mathrm{Vol}(V_{n,\alpha})}{\mathrm{Vol}(V_n)}$, where $\mathrm{Vol}\,(V_n) = \frac{2^n}{n!}\prod_{i=1}^{n}\left(\frac{2i}{2i-1}\right)^{n+1-i}$.

In a sense, $P_n(\alpha)$ should be similar in behaviour to the number of curves X genus g, satisfying the inequality $\frac{(q+1)-\#X(\mathbb{F}_q)}{\sqrt{q}} \geq \alpha$, provided that the isogeny classes of Jacobians are "*randomly distributed*" in the set of isogeny classes of abelian varieties.

Finally, we can formulate our first task as follows: study the $P_n(\alpha)$ as a function of α for some fixed n. Now, we illustrate this idea by several examples.

4.1 Calculations and examples.

4.1.1 Elliptic curves

First of all, we consider the simple case $g = 1$. If $g = n = 1$ then $C_\alpha = [\alpha; 2]$. For any $r \in C_\alpha$, consider the polynomial $x^2 - rx + 1$. We see that $b_1 = -r$ and $|\,\mathrm{Vol}(V_\alpha)| = 2 - \alpha$. Thus $P_1(\alpha) = \frac{2-\alpha}{4}$.

It is interesting to compare this result with the following theorem:

Theorem 7. *The set of isogeny classes of elliptic curves E over $\mathbb{F}_q$ is bijective equal to the set of integer m, such that $|m| \leq 2\sqrt{q}$, and one of the following conditions holds:*

1. $(q, m) = 1$;
2. *if q is square, then $m = \pm 2\sqrt{q}$;*
3. *if q is square and $p \neq 1 \mod (3)$, then $m = \pm\sqrt{q}$;*
4. *if q is not square and $p = 2$ or $p = 3$, then $m = \pm\sqrt{pq}$*
5. *if q is not square, then $m=0$; or q is square and $p \neq 1 \mod 4$, $m=0$.*

Herewith, $\#E(k) = q + 1 - m$.

Definition 6. Define M_α as the number of isogeny classes of eliptic curves X, such that $q + 1 - \#X(k) \geq \alpha\sqrt{q}$.

By using the above theorem, one can conclude that

$$\left| M_\alpha - \sqrt{q}(2-\alpha)(1-\frac{1}{p}) \right| \leq 6.$$

And we see that $\frac{M_\alpha}{4\sqrt{q}} \to P(\alpha)$ if and only if $p \to \infty$.

4.1.2 The case $g = 2$

Here, have $\Phi\ (r_1, r_2) = (b_1, b_2)$, where b_1, b_2 are defined by the equation:

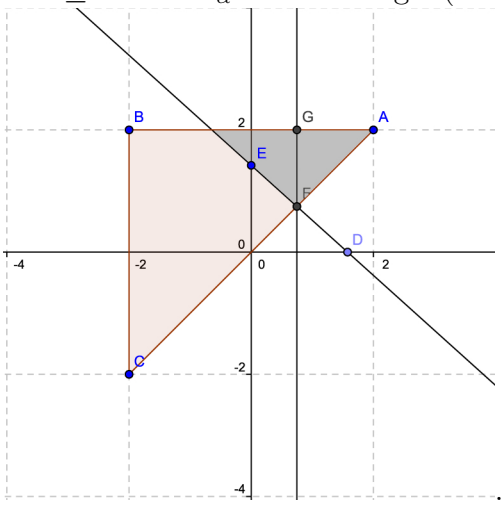
$$(x^2 - r_1 x + 1)(x^2 - r_2 x + 1) = x^4 - b_1(x^3 + x) + b_2 x^2 + 1.$$

It is easy to see that $b_1 = -r_1 - r_2$ and $b_2 = 2 + r_1 r_2$. Hence, $\det(d\Phi) = r_2 - r_1$.

For brevity, we change the variables: $x = r_1$ and $y = r_2$. So, we have to calculate the integral: $\int_{C_\alpha}(y - x) = I$, where C_α is the intersection of the triangle C_2 and the half-plane $x + y \geq \alpha$.

There are two different cases: $\alpha \geq 0$ and $\alpha \leq 0$.

If $\alpha \geq 0$ then C_α is the triangle (see the picture).



So, $I = I_1 + I_2$, where I_1 is the integral over the triangle for x such that $2 - \alpha \leq x \leq \frac{\alpha}{2}$, and I_2 is the same integral for $\frac{\alpha}{2} \leq x \leq 2$.

$$I_1 = \int_{\alpha-2}^{\frac{\alpha}{2}} \int_{\alpha-x}^{2} (y - x)dydx = \frac{1}{16}(\alpha - 4)(11\alpha^2 - 4\alpha(3\alpha - 4) - 8\alpha - 16) =$$

$$= -\frac{1}{16}(\alpha - 4)^3.$$

Similarly:

$$I_2 = \int_{\frac{\alpha}{2}}^{2} \int_{x}^{2} (y - x)dydx = \int_{\frac{\alpha}{2}}^{2} \frac{(x-2)^2}{2}dx = -\frac{1}{48}(\alpha - 4)^3.$$

As a result: $I = -\frac{1}{16}(\alpha - 4)^3 - \frac{1}{48}(\alpha - 4)^3 = -\frac{1}{12}(\alpha - 4)^3$.

Take now the case $\alpha \leq 0$:

$$I = V_2 - \int_{-2}^{\frac{\alpha}{2}} \int_{x}^{\alpha - x} (y - x) dy dx = V_2 - \int_{-2}^{\frac{\alpha}{2}} \frac{(\alpha - 2x)^2}{2} dx = V_2 - \frac{(\alpha + 4)^3}{12}.$$

Summing up,

$$P_2(\alpha) = \begin{cases} -\frac{1}{12}(\alpha - 4)^3 \frac{3}{32} = \frac{1}{2^7}(4 - \alpha)^3, & \text{if } \alpha \geq 0; \\ 1 - \frac{1}{2^7}(\alpha + 4)^3, & \text{if } \alpha \leq 0. \end{cases}$$

Note that if $\alpha = 0$, then both sides are equal.
It is interesting to compare this result with theorem 1.2 in [4].

4.1.3 The case g=3

Here, we have to calculate the integral

$$I = \int_{C_\alpha} (x_3 - x_2)(x_3 - x_1)(x_2 - x_1)\ dx_1\ dx_2\ dx_3.$$

There are 3 different cases: $\alpha \in [6 - 4(k+1); 6 - 4k]$, $k = 0$,1 or 2.
If $k = 0$, we have

$$I = \int_{\frac{\alpha}{3}}^{2} \int_{\frac{\alpha - x_3}{2}}^{x_3} \int_{\alpha - x_3 - x_2}^{x_2} (x_2 - x_1)(x_3 - x_2)(x_3 - x_1)\ dx\ dy\ dz = \frac{1}{2880}(\alpha - 6)^6.$$

At the same time, $\mathrm{Vol}(V_3) = \frac{2^3}{3!}\left(\frac{2}{1}\right)^3\left(\frac{4}{3}\right)^2\left(\frac{6}{5}\right)^1 = \frac{2^{10}}{3^2 5}$.
Hence, if $\alpha \in [2; 6]$, then $P_3(\alpha) = \frac{1}{2^{16}}(\alpha - 6)^6$.
Similarly, if $\alpha \in [-6; -2]$, then $P_3(\alpha) = 1 - \frac{1}{2^{16}}(\alpha + 6)^6$.

Consider the more difficult case $-2 \leq \alpha \leq 2$. Let us denote $g(\alpha) = \mathrm{Vol}(V_3)P'(\alpha)$. By definition, we have:

$$g(\alpha) = \mathrm{Vol}(V_3) \lim_{h \to \infty} \frac{P(\alpha + h) - P(\alpha)}{h} = \int_{\hat{C}_\alpha} (x_3 - x_2)(x_3 - x_1)(x_2 - x_1),$$

where $\hat{C}_\alpha$ is the intersection of C_3 and plane $x_1 + x_2 + x_3 = \alpha$.
We have

$$\hat{C}_\alpha = \begin{cases} 2 - x_3 \geq 0; \\ x_3 - x_2 \geq 0; \\ x_2 - x_1 \geq 0; \\ x_1 + 2 \geq 0; \\ x_1 + x_2 + x_3 = \alpha. \end{cases}$$

Change the variables: $z = 3(2 - x_3)$, $y = 2(x_3 - x_2)$, $x = x_2 - x_1$. Then :

$$\hat{C}_\alpha = \begin{cases} z \geq 0; \\ y \geq 0; \\ x \geq 0; \\ 4 - \frac{z}{3} - \frac{y}{2} - x \geq 0; \\ x + y + z = 6 - \alpha. \end{cases} \quad \text{or} \quad \hat{C}_\alpha = \begin{cases} 6 - \alpha - x - y \geq 0; \\ y \geq 0; \\ x \geq 0; \\ 2\alpha + 12 \geq 4x + y. \end{cases}$$

Thus, we have

$$g(\alpha) = \frac{1}{6} \int_0^{\alpha+2} \int_0^{6-\alpha-x} \frac{y}{2} x \left(\frac{y}{2} + x \right) \, dy \, dx + \frac{1}{6} \int_{\alpha+2}^{\frac{\alpha+6}{2}} \int_0^{2\alpha+12-4x} \frac{y}{2} x \left(\frac{y}{2} + x \right) \, dy \, dx =$$

$$= \frac{1}{6} \left(\frac{1}{240} (2+\alpha)^2 (1864 - 1284\alpha + 198\alpha^2 + 13\alpha^3) - \frac{1}{240} (-2+\alpha)^3 (292 + 148\alpha + 13\alpha^2) \right) =$$

$$= \frac{1}{120} (816 - 200\alpha^2 + 15\alpha^4).$$

Hence, $P(\alpha) = \left(\frac{a^5}{40} - \frac{5a^3}{9} + \frac{34\alpha}{5} \right) \frac{1}{\text{Vol}(V_3)} + C = \frac{9}{8192}\alpha^5 - \frac{25}{1024}\alpha^3 + \frac{153}{512}\alpha + C$.
Since, $P(2) = P(2)$ we obtain:

$$\frac{1}{2^{16}} (4)^6 = \frac{7}{16} + C.$$

So, $C = -\frac{6}{16}$ and $P(\alpha) = \frac{9}{8192}\alpha^5 - \frac{25}{1024}\alpha^3 + \frac{153}{512}\alpha - \frac{3}{8}$.
Summing up,

$$P_3(\alpha) = \begin{cases} \frac{1}{2^{16}} (\alpha - 6)^6, & \text{if } 2 \leq \alpha \leq 6; \\ \frac{9}{8192}\alpha^5 - \frac{25}{1024}\alpha^3 + \frac{153}{512}\alpha - \frac{3}{8}, & \text{if } -2 \leq \alpha \leq 2; \\ 1 - \frac{1}{2^{16}} (\alpha + 6)^6, & \text{if } -6 \leq \alpha \leq -2. \end{cases}$$

Unfortunately, in the case genus$(X) = 3$ there is no exact description of the isogeny classes of Jacobians of curves X. Thus, we can not compare our result with the other.

4.2 The main results.

Proposition 2. *The function $P_n(\alpha)$ is monotonic and continuous on the interval $[-2n; 2n]$.*

Proof. Consider the derivative $P'(\alpha) = \lim\limits_{h\to 0} \frac{P(\alpha+h)-P(\alpha)}{h} = \int_{\hat{C}_\alpha} \prod(x_i - x_j)$, where $\hat{C}_\alpha$ is the intersection of C_n and the hyperplane $\sum x_i = \alpha$. On can see that this integral is well defined and nonnegative everywhere. Therefore, $P(\alpha)$ is a differentiable function with $P'(\alpha) \geq 0$. □

Proposition 3. *On each interval $[2n - 4k; 2n - 4(k + 1)]$, $k = 0, \ldots, n - 1$ $P_n(\alpha)$ is a polynomial of degree $d \leq \frac{n(n+1)}{2}$.*

Proof. The function $P(\alpha)$ is a polynomial until the hyperplane $\sum x_i = \alpha$ passes through a vertex of C_n. It easy to see that, all of C_n vertices are $c_k = (-2; \ldots, -2, 2, \ldots, 2)$. Thus, the type of the intersection of hyperplane and C_n changes only when $\alpha = 2n - 4k$, $k \in \mathbb{Z}$,$k \geq 0$.

If $\alpha \in [2n - 4k; 2n - 4(k + 1)]$ then we have to integrate the polynomial of degree $\frac{n(n-1)}{2}$ over the n dimensional polytopes. It is easy to see, that this integral is a polynomial of degree $d \leq \frac{n(n-1)}{2} + n = \frac{n(n+1)}{2}$.

□

Proposition 4. *Define S_α as the set of all points x in $\mathbb{R}^n$, such that $x_i \geq 0$ and $\sum x_i \leq \alpha$. Then:*

$$\int_{S_\alpha} x_1^{k_1} \ldots x_n^{k_n} = \frac{k_1!k_2! \ldots k_n!}{(\sum k_i + n)!} \alpha^{k_1+k_2+\cdots+k_n+n}.$$

Proof. Is an easy calculation we leave to the reader. □

Proposition 5. *If $\alpha \in [2n - 4; 2n]$, then $P_n(\alpha) = C(2n - \alpha)^{\frac{n(n+1)}{2}}$, where C is some constant.*

Proof. Change the variables $y_k = \frac{1}{k}(x_{k+1} - x_k)$ if $k < n$, and $y_n = \frac{1}{n}(2 - x_n)$. Then:

1. if $-2 \leq x_1 \leq \cdots \leq x_n \leq 2$, then $y_k \geq 0$;
2. if $\sum x_i \geq \alpha$, then $\sum y_i \leq (2n - \alpha)$;
3. $\prod\limits_{1 \leq j < i \leq n} (x_i - x_j) = \prod\limits_{1 \leq j < i \leq n} \left(\sum\limits_{m=j}^{m=i-1} m y_m \right)$.

Define $S_\alpha = \{y \in \mathbb{R}^n | y_k \geq 0 \text{ and } \sum y_k \leq (2n - \alpha)\}$ Then:

$$\int_{C_{n,\alpha}} \prod_{1 \leq j < i \leq n} (x_i - x_j) = n! \int_{S_\alpha} \prod_{1 \leq j < i \leq n} \left(\sum_{m=j}^{m=i-1} m y_m \right)$$

Now $\prod\limits_{1 \leq j < i \leq n} \left(\sum\limits_{m=j}^{m=i-1} m y_m \right) = \sum c_{k_1,k_2,\ldots k_n} y_1^{k_1} \ldots y_n^{k_n}$, where $c_{k_1,k_2,\ldots k_n}$ is some constant and $\sum k_i = \frac{n(n-1)}{2}$.

So, by using the above facts and proposition 4, we obtain the proof.

□

Proposition 6. $P_n(\alpha) = 1 - P_n(-\alpha)$.

Proof. $P_n(\alpha) + P_n(-\alpha) = \frac{\mathrm{Vol}(V_n)}{\mathrm{Vol}(V_n)} = 1$. □

5 On abelian varieties with many points

5.1 General setting

As before, we have that if A is an abelian variety and $k = \mathbb{F}_q$, then

$$\#A(k) = f_A(1) = \prod_{i=1}^{2n} (1 - \alpha_i) = \prod_{i=1}^{n} (q + 1 - x_i \sqrt{q}),$$

where $-2 \leq x_i \leq 2$ and $n = \dim(A)$.

Hence,

$$\#A(k) - (q+1)^n =$$

$$= (q+1)^{n-1} \sqrt{q} \left(- \sum x_i \right) + (q+1)^{n-2} q \left(\sum_{n \geq i > j \geq 1} x_i x_j \right) + \cdots + (-1)^n q^{\frac{n}{2}} x_1 \ldots x_n.$$

Let us fix the isogeny classes of abelian varieties A and some number $q = p^k$ (p is prime). Change the variable $x \to \sqrt{q} x$. Consider a few definitions:

Definition 7. Define $R_n(x,q) = \#A(k) - (q+1)^n - (q+1)^{n-1}(-\sum x_i)$.

Then:

$$\frac{(q+1)^n - \#A(k)}{(q+1)^{n-1}} = \sum x_i - \frac{R_{n,q}}{(q+1)^{n-1}}.$$

For brevity, almost everywhere below, we will omit the index n.

Definition 8. Define $S_{\alpha,q} = \{x \in C_n \mid \sum x_i - \frac{R_{n,q}}{(q+1)^{n-1}} \geq \alpha\}$.

Definition 9. Define $T_{\alpha,q} = \Phi(S_{\alpha,q})$, for definition Φ see page 6.

So, the integer points in $T_{\alpha,q}$ contain the points which correspond to the isogeny classes of abelian varieties A with dimension n and satisfying the inequality:

$$(q+1)^n - \#A(k) \geq (q+1)^{n-\frac{1}{2}}\alpha.$$

As before, we would like to calculate the volume of $T_{\alpha,q}$.

Definition 10. $F_{n,q}(\alpha) = \frac{1}{\mathrm{Vol}(V_n)} \int_{S_\alpha} \prod(x_i - x_j) dx_1 \ \ldots \ dx_n$.

5.2 Examples

5.2.1 n=1

If $n = 1$, then A is elliptic curve and we have $f(1) = q + 1 - x\sqrt{q}$, where $-2 \leq x \leq 2$. Then $F_{1,q}(\alpha) = P(1,\alpha) = \frac{2-\alpha}{4}$. It is trivial.

5.2.2 n=2

If $n = 2$, then A is 2-dimensional abelian variety. Here we have: $\#A(k) = (q + 1 - x\sqrt{q})(q + 1 - y\sqrt{q})$, where $-2 \leq x \leq y \leq 2$. Then:

$$\frac{(q+1)^2 - \#A}{q\sqrt{q}} = x + y - xy\frac{1}{\sqrt{q}}.$$

We see, that as $q \to \infty$, then the right-hand side tends to $x + y$. Thus, $\lim\limits_{q\to\infty} F_{2,q}(\alpha) = P(\alpha)$. The similar result is true for any n.

Proposition 7. $\lim\limits_{q\to\infty} F_{n,q}(\alpha) = P_n(\alpha)$.

Proof. Let $H_{\alpha,q} = \{x \in C_n \mid \ (\sum x_i - \alpha) \leq |\frac{R_{n,q}}{q^{n-\frac{1}{2}}}|\}$,$C_1 = \text{Vol}(V_n)$ and $C_2 = \max_{x \in C_n} (\prod (x_i - x_j))$. Then:

$$|F_{n,q}(\alpha) - P(\alpha)| \leq C_1^{-1} \, | \int_{H_{\alpha,q}} \prod (x_i - x_j) dx_1 \, \ldots \, dx_n | \leq C_1^{-1} C_2 \, \text{Vol}\,(C_n) \, \text{Vol}\,(H_{\alpha,q}) \, .$$

But, $\text{Vol}\,(H_{\alpha,q}) \to 0$, as $q \to \infty$.

□

Contents

References

[1] Stephen A. Dipippo and Everett W. Howe "Real polynomials with all roots on the unit circle and abelian varieties over finite fields".

[2] H. Stichtenoth:"Algebraic Function Fields and Codes", Springer, 1993-6-25 - 260.

[3] C. Ritzenthaler "Curves over finite fields", Lecture notes.

[4] C. Ritzenthaler "Jacobians of genus 2 over finite fields".

[5] J.Milne "Abelian varieties", Lecture notes.