

Dependent rational points on curves over finite fields - Lefschetz theorems and exponential sums

Abstract

For an algebraic curve defined over \mathbb{F}_q we study the probability that τ randomly chosen \mathbb{F}_q -rational points on the curve impose dependent conditions on the functions in a given τ -dimensional vector space of rational functions on the curve. This probability tends to be close to $\frac{1}{q}$.

The results have applications in the assessment of the performance of decoding algorithms for algebraic geometry codes.

The proofs involve a geometric construction, Lefschetz theorem for quasi-projective varieties and majorizations of exponential sums.

Key words: Newton polyhedra, exponential sums, Lefschetz theorem, Points failing to impose independent conditions, (Error-correcting Codes, decoding), 14F20, 14G10, 14G15, 14H25, (94B27), (94B35)

1 Introduction

Let p be a prime number, let \mathbb{F}_q be the finite field with q elements and with $\text{char}(\mathbb{F}_q) = p$. Let $k = \overline{\mathbb{F}_q}$ be an algebraic closure. Let \mathbb{G}_m denote the multiplicative group of k .

For an algebraic curve defined over \mathbb{F}_q we study the probability that τ randomly chosen \mathbb{F}_q -rational points on the curve impose dependent conditions on

¹ This work was done while the author visited: Équipe “Arithemétique et Théorie de l’Information” Institut de Mathématique de Luminy. The author would very much like to express his gratitude to the Équipe and to the Institut de Mathématique de Luminy. FRANCE

² E-mail: matjph@imf.au.dk

the functions in a given τ -dimensional vectorspace of rational functions on the curve. This probability tends to be close to $\frac{1}{q}$. We obtain two such results.

The results have applications in the assessment of the performance of decoding algorithms for algebraic geometry codes according to [JNH].

In section 2, we recall the asymptotic result that the probability converges to $\frac{1}{q^\tau}$ for larger and larger field extensions \mathbb{F}_{q^i} of the ground field \mathbb{F}_q . This result is obtained in [H-L] with G. Lachaud for smooth, projective curves C and vectorspaces of functions of the form $L(D)$, where D is a divisor on the curve with $\deg D \geq 2g + 1$.

The proof is based on a geometric construction and a Lefschetz theorem for quasi-projective smooth varieties.

In section 3, the same geometric construction is used in a different setup, namely where C^* is a curve in a torus $\mathbb{G}_m \times \mathbb{G}_m$, with no restrictions on smoothness and irreducibility. The difference between the sought probability and $\frac{1}{q}$ is expressed as an exponential sum on a subvariety of a torus $\mathbb{G}_m \times \cdots \times \mathbb{G}_m$. The works of A. Adolphson and S. Sperber [A-S] allow us to determine explicit majorisations for the exponential sums.

2 Asymptotic result - Lefschetz Theorems

Let C be a smooth and absolutely irreducible curve of genus g defined over the finite field \mathbb{F}_q and let D be a \mathbb{F}_q -rational divisor on C with $l(D) = \tau$.

Let X be τ -tuples of pairwise different points on C , i.e.

$$X = \{(P_1, \dots, P_\tau) \mid P_i \neq P_j \text{ for } i \neq j\}$$

and let $\Gamma \subseteq X$ be τ -tuples of pairwise different points on C failing to impose independent conditions on the linear system of divisors equivalent to D . Specifically, if $\overline{\mathbb{F}}_q(C)$ denotes the field of rational functions on C , then

$$\Gamma = \{(P_1, \dots, P_\tau) \in X \mid \exists f \in \overline{\mathbb{F}}_q(C) : \operatorname{div}(f) + D - (P_1 + \dots + P_\tau) \geq 0\}.$$

Let $|X(\mathbb{F}_{q^j})|$ and $|\Gamma(\mathbb{F}_{q^j})|$ denote the number of \mathbb{F}_{q^j} -rational points on X and Γ .

With G. Lachaud we obtain in [H-L] the following theorem. As the geometric construction in the proof is also used in section 3, we recollect the proof of the theorem.

Theorem 1 *In the notation above assume that $\deg(D) \geq 2g + 1$ and let $\tau = \deg(D) + 1 - g$. Assume that $\Gamma \neq \emptyset$. There is a constant c (independent of j), such that*

$$\left| |X(\mathbb{F}_{q^j})| - q^j |\Gamma(\mathbb{F}_{q^j})| \right| \leq c (q^j)^{\frac{\tau+1}{2}}. \quad (1)$$

The bounding term $c (q^j)^{\frac{\tau+1}{2}}$ cannot in general be replaced by a smaller power of q^j .

Example 2 *Let C be an elliptic curve with $|C(\mathbb{F}_q)| = 1 + q$ and let $D = 3P_0$. Then $\tau = 3$ and Γ are triples of collinear points on C . In this case we have*

$$|X(\mathbb{F}_q)| = |C(\mathbb{F}_q)|(|C(\mathbb{F}_q)| - 1)(|C(\mathbb{F}_q)| - 2) = q^3 - q$$

$$|\Gamma(\mathbb{F}_q)| = (|C(\mathbb{F}_q)| - 9)(|C(\mathbb{F}_q)| - 1 - 4) = (q - 8)(q - 4) = q^2 - 12q + 32$$

assuming that the 2-torsion and 3-torsion points are \mathbb{F}_q -rational. This follows from the fact that 3 points on C are collinear if and only if they have sum 0 in the group structure on the elliptic curve. We now have for all odd j , that

$$|X(\mathbb{F}_{q^j})| - q |\Gamma(\mathbb{F}_{q^j})| = -12(q^j)^2 - 36q^j.$$

Central to the proof of the theorem is the following lemma, which is obtained through a geometric construction.

Lemma 3 *In the notation above*

- i) $X \setminus \Gamma$ is affine.*
- ii) Γ is smooth if $\deg(D) \geq 2g + 1$*

PROOF. Let $(a_{i,1} : \dots : a_{i,\tau})$ be homogeneous coordinates on the i 'th copy of $\mathbb{P}^{\tau-1}$ in $\mathbb{P}^{\tau-1} \times \dots \times \mathbb{P}^{\tau-1}$ and let $V \subseteq \mathbb{P}^{\tau-1} \times \dots \times \mathbb{P}^{\tau-1}$ be the closed subscheme defined by the vanishing of the determinant

$$\begin{vmatrix} a_{1,1} & \dots & a_{\tau,1} \\ a_{1,2} & \dots & a_{\tau,2} \\ \dots & \dots & \dots \\ a_{1,\tau} & \dots & a_{\tau,\tau} \end{vmatrix}$$

Consider for a moment the Segre embedding

$$\overbrace{\mathbb{P}^{\tau-1} \times \dots \times \mathbb{P}^{\tau-1}}^{\tau\text{-fold}} \xrightarrow{\text{Segre}} \mathbb{P}^N, \quad N = \tau! - 1$$

the morphism defined by

$$(a_{1,1} : \dots : a_{1,\tau}) \times \dots \times (a_{\tau,1} : \dots : a_{\tau,\tau}) \mapsto (\dots : a_{1,i_1} \cdot a_{2,i_2} \cdot \dots \cdot a_{\tau,i_\tau} : \dots).$$

Then we see that $V \subseteq \mathbb{P}^{\tau-1} \times \dots \times \mathbb{P}^{\tau-1}$ is the inverse image of a hyperplane $H \in \mathbb{P}^N$.

The assumption $\deg(D) \geq 2g + 1$ implies that $\tau = l(D) = \deg(D) + 1 - g$ by Riemann-Roch, and the divisor D defines an embedding of the curve C as a smooth curve in $\mathbb{P}^{\tau-1}$:

$$\phi : C \rightarrow \mathbb{P}^{\tau-1}.$$

By the definition of X and Γ , we have that (P_1, \dots, P_τ) is in Γ if and only if $\phi(P_1), \dots, \phi(P_\tau)$ are linearly dependent in \mathbb{P}^τ , equivalently lie in a hyperplane $L \subset \mathbb{P}^\tau$, therefore we have the cartesian diagrams of intersections:

$$\begin{array}{ccccccc} X & \longrightarrow & \overbrace{C \times \dots \times C}^{\tau\text{-fold}} & \xrightarrow{\phi \times \dots \times \phi} & \overbrace{\mathbb{P}^{\tau-1} \times \dots \times \mathbb{P}^{\tau-1}}^{\tau\text{-fold}} & \xrightarrow{\text{Segre}} & \mathbb{P}^N \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ \Gamma & \longrightarrow & (\phi \times \dots \times \phi)^{-1}(V) & \longrightarrow & V & \longrightarrow & H \end{array}$$

and we note the important fact that

$$X \setminus \Gamma = \overbrace{C \times \dots \times C}^{\tau\text{-fold}} \setminus (\phi \times \dots \times \phi)^{-1}(V).$$

It follows that $X \setminus \Gamma$ is isomorphic to the complement of a hyperplane section in a projective variety and therefore affine, which was the first assertion.

As for assertion on smoothness, assume to the contrary that $(P_1, \dots, P_\tau) \in \Gamma$ is a singular point on Γ , this implies that H (and thereby V) do not intersect X transversally at (P_1, \dots, P_τ) .

Let L be a hyperplane in $\mathbb{P}^{\tau-1}$ through P_1, \dots, P_τ which exists as $(P_1, \dots, P_\tau) \in \Gamma$. All τ -tuples of points in L are linearly dependent, i.e. for all j , therefore we have

$$L_j := P_1 \times \dots \times P_{j-1} \times L \times P_{j+1} \times \dots \times P_\tau \subseteq V \subseteq \mathbb{P}^{\tau-1} \times \dots \times \mathbb{P}^{\tau-1}.$$

Consider the Cartesian diagrams of intersections in $\mathbb{P}^{\tau-1} \times \dots \times \mathbb{P}^{\tau-1}$:

$$\begin{array}{ccc} X & \longrightarrow & \mathbb{P}^{\tau-1} \times \dots \times \mathbb{P}^{\tau-1} \\ \uparrow & & \uparrow \\ \Gamma & \longrightarrow & V \\ \uparrow & & \uparrow \\ P_1 \times \dots \times P_{j-1} \times L \cap C \times P_{j+1} \times \dots \times P_\tau & \longrightarrow & L_j \end{array}$$

As the intersection between X and V is not transversal at (P_1, \dots, P_τ) , the intersection between X and $P_1 \times \dots \times P_{j-1} \times L \times P_{j+1} \times \dots \times P_\tau$ cannot be either, consequently L is a tangent hyperplane to the curve C at P_j . This is true for all P_1, \dots, P_τ , i.e. , there exists a rational function in $L(D)$ vanishing to at least second order at P_1, \dots, P_τ , therefore $l(D - (2P_1 + \dots + 2P_\tau)) > 0$. However, this contradicts the assumption, as

$$\begin{aligned} \deg(D - (2P_1 + \dots + 2P_\tau)) &= \deg(D) - 2l(D) = \\ \deg(D) - 2(\deg(D) + 1 - g) &= 2g - 2 - \deg(D) < 0. \end{aligned}$$

Assume that the prime l is different from the characteristic of the ground field. Let \mathbb{Q}_l denote the l -adic numbers. For a constructible sheaf \mathcal{F} of \mathbb{Q}_l -vector spaces let $H^i(X, \mathcal{F})$ (resp. $H_c^i(X, \mathcal{F})$) denote the étale l -adic cohomology groups (resp. the étale l -adic cohomology groups with compact support), see [M].

Finally, for an integer c we denote by $\mathcal{F}(c)$ the Tate twist of \mathcal{F} and

$$H^i(X, \mathcal{O}_l(c)) = H^i(X, \mathcal{O}_l(c)) \otimes \mathcal{O}_l(c)$$

The second main ingredient in the proof is a Lefschetz Theorem for quasi-projective varieties. We have not been able to find a reference for it and give a proof along the lines of [J, Corollaire 7.2], see also [G-L] for related results.

Lemma 4 A Lefschetz Theorem for quasi-projective varieties. *Let $X \subset \mathbb{P}^N$ be a quasi-projective, smooth scheme of dimension n and let $Y = X \cap H$ be a smooth hyperplane section, such that $X \setminus Y$ is affine. Then there are isomorphisms:*

$$H_c^{i-2}(Y, \mathbb{Q}_l(-1)) \rightarrow H_c^i(X, \mathbb{Q}_l)$$

for $i \geq n + 2$.

PROOF. For any locally constant sheaf \mathcal{F} of $\mathbb{Z}/(l)$ -modules, the inverse image morphisms:

$$H^i(X, \mathcal{F}) \rightarrow H^i(Y, \mathcal{F}) \tag{2}$$

are isomorphisms for $i \leq n - 2$ as follows from the long exact cohomology sequence using the assumption that $X \setminus Y$ is affine. As both X and Y are assumed to be smooth, Poincaré duality applied to (2) gives the result.

PROOF. (Of Theorem 1). The ground field is the finite field \mathbb{F}_q and $H_c^i(X, \mathcal{O}_l)$ is endowed with an action of the Frobenius morphism **Frob**. The Lefschetz

trace formula [M, p.292] by A. Grothendieck determines the number of \mathbb{F}_q -rational points in terms of the traces of **Frob** on the étale cohomology spaces.

We have accordingly

$$|X(\mathbb{F}_q)| = \sum_{i=0}^{2\tau} (-1)^i \text{Tr}(\mathbf{Frob} | H_c^i(X, \mathbb{Q}_l)) \quad (3)$$

$$q |\Gamma(\mathbb{F}_q)| = q \sum_{i=0}^{2\tau-2} (-1)^i \text{Tr}(\mathbf{Frob} | H_c^i(\Gamma, \mathbb{Q}_l)) \quad (4)$$

As for the high dimensions, we obtain from Lemma 4 applied to X and Γ , that

$$\begin{aligned} q \sum_{i=\tau}^{2\tau-2} (-1)^i \text{Tr}(\mathbf{Frob} | H_c^i(\Gamma, \mathbb{Q}_l)) &= \\ \sum_{i=\tau}^{2\tau-2} (-1)^i \text{Tr}(\mathbf{Frob} | H_c^i(\Gamma, \mathbb{Q}_l(-1))) &= \\ \sum_{i=\tau+2}^{2\tau} (-1)^i \text{Tr}(\mathbf{Frob} | H_c^i(X, \mathbb{Q}_l)) & \end{aligned}$$

Combining this with (3) and (4) one has:

$$\begin{aligned} |X(\mathbb{F}_q)| - q |\Gamma(\mathbb{F}_q)| &= \\ \sum_{i=0}^{\tau+1} (-1)^i \text{Tr}(\mathbf{Frob} | H_c^i(X, \mathbb{Q}_l)) - & \\ q \sum_{i=0}^{\tau-1} (-1)^i \text{Tr}(\mathbf{Frob} | H_c^i(\Gamma, \mathbb{Q}_l)) & \end{aligned}$$

Deligne's main theorem [D] gives that the eigenvalues of **Frob**'s action on the i 'th cohomology group have absolute values $\leq q^{\frac{i}{2}}$. This immediately implies (5) of Theorem 1 as the dimensions on the cohomology groups do not depend on the power j of q and the highest power of q being $q^{\frac{\tau+1}{2}}$.

3 Curves in a two-dimensional Torus. Exponential sums

In this section we will be concerned with subvarieties $C^* \subset (\mathbb{G}_m)^2$ defined over \mathbb{F}_q , with no restrictions on smoothness and irreducibility, and exponential sums.

The probability that τ randomly chosen \mathbb{F}_q -rational points on the curve impose dependent conditions on the functions in a given τ -dimensional vectorspace of rational functions on the curve is close to $\frac{1}{q}$. In fact, the difference between the

sought probability and $\frac{1}{q}$ is expressed as an exponential sum on a subvariety of a torus $\mathbb{G}_m \times \cdots \times \mathbb{G}_m$. The works of A. Adolphson and S. Sperber [A-S] allow to determine explicit majorisations for the exponential sums, bounding the difference between the sought probability and $\frac{1}{q}$.

3.1 Exponential sums

Let $V \subseteq (\mathbb{G}_m)^r \times \mathbb{A}^s$ be a subvariety defined over \mathbb{F}_q . Set $n = r + s$.

Let

$$G = \sum_{j \in J} a_j X^j \in \mathbb{F}_q[X_1, \dots, X_n, (X_1 \cdots X_r)^{-1}]$$

be a regular function on V , where the sum is over a finite subset J and we assume that $a_j \neq 0$ for all $j \in J$.

The *Newton polyhedron* $\Delta(G)$ of G is the convex hull in \mathbb{R}^n of the set $J \cup \{(0, \dots, 0)\}$. Let $\text{vol}(G)$ be the volume of $\Delta(G)$ with respect to Lebesgue measure on \mathbb{R}^n .

Let $S_2 = \{r + 1, \dots, n\}$. For each $B \subseteq S_2$, let $\mathbb{R}_B^n = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid x_i = 0 \text{ if } i \in B\}$ and let $\text{vol}_B(G)$ be the volume of $\Delta(G) \cap \mathbb{R}_B^n$ with respect to Lebesgue measure on \mathbb{R}_B^n . Finally, set

$$\nu_{S_2}(G) = \sum_{B \subseteq S_2} (-1)^{|B|} (n - |B|)! \text{vol}_B(G) \quad (5)$$

For a face σ (of any dimension) of $\Delta(G)$, set

$$G_\sigma = \sum_{j \in \sigma \cap J} a_j X^j.$$

The function G is *nondegenerate* if for every face σ of $\Delta(G)$ that does not contain the origin, the polynomials $\frac{\delta G}{\delta X_1}, \dots, \frac{\delta G}{\delta X_n}$ have no common zero in $(k^*)^n$. The function G is *commode* if for all subsets $B \subseteq S_2$, $\dim \Delta_{G_B} = \dim \Delta_{G_{S_2}} + |S_2 - B|$, where G_B is the polynomial obtained from G by substituting $X_i = 0$ for all $i \in B$.

Let $\chi : \mathbb{F}_q \rightarrow \mathbb{C}^*$ be a nontrivial additive character on \mathbb{F}_q and set

$$S(V, G) = \sum_{x \in V(\mathbb{F}_q)} \chi(G(x)).$$

A. Adolphson and S. Sperber determine explicit majorisations for certain exponential sums. There is a set \mathcal{S}_Δ consisting of all but finitely many prime

numbers associated to the Newton polyhedron. This set can be effectively determined, see [A-S] (proof of LEMMA 4.4).

Theorem 5 ([A-S], THEOREM 4.20) *If $\text{char}(k) \in \mathcal{S}_\Delta$ and G is nondegenerate and commode, then*

$$|S((\mathbb{G}_m)^r \times \mathbb{A}^s, G)| \leq \nu_{S_2}(G)\sqrt{q}$$

Besides this result we will need a result that relates a certain exponential sum, the number of \mathbb{F}_q -rational points on a variety $V \subseteq (\mathbb{G}_m)^n$ defined by *homogeneous* equations over \mathbb{F}_q and the number of \mathbb{F}_q -rational points on a hyperplane section $V_G := V \cap \{G = 0\}$ for $G \in \mathbb{F}_q[X_1, \dots, X_n]$ *homogeneous*, see also [Sh-Sk,Sk].

Lemma 6 *Let $V \subseteq (\mathbb{G}_m)^n$ be defined by homogeneous equations over \mathbb{F}_q and let $G \in \mathbb{F}_q[X_1, \dots, X_n]$ homogeneous of degree d . Assume that $q - 1$ and d are coprime. Then*

$$(q - 1)S(V, G) = q(|V_G(\mathbb{F}_q)| - |V(\mathbb{F}_q)|).$$

PROOF. As V is defined by homogeneous equations, the mapping

$$\mathbb{F}_q^* \times V(\mathbb{F}_q) \rightarrow V(\mathbb{F}_q), (t, x) \mapsto tx$$

is a $(q - 1)$ -fold covering of $V(\mathbb{F}_q)$. Therefore

$$\begin{aligned} S(V, G) &= \sum_{x \in V(\mathbb{F}_q)} \chi(G(x)) = \frac{1}{q - 1} \sum_{t \in \mathbb{F}_q^*} \sum_{x \in V(\mathbb{F}_q)} \chi(G(tx)) = \\ &= \frac{1}{q - 1} \left[\sum_{t \in \mathbb{F}_q^*} \sum_{x \in V(\mathbb{F}_q)} \chi(G(tx)) - \sum_{x \in V(\mathbb{F}_q)} \chi(G(0, \dots, 0)) \right] = \\ &= \frac{1}{q - 1} \left[\sum_{t \in \mathbb{F}_q^*} \sum_{x \in V(\mathbb{F}_q)} \chi(t^d G(x)) - |V(\mathbb{F}_q)| \right] = \\ &= \frac{1}{q - 1} [q |V_G(\mathbb{F}_q)| - |V(\mathbb{F}_q)|] \end{aligned}$$

by orthogonality of characters, as d is coprime to $q - 1$.

3.2 Curves in a two-dimensional torus

Let $C = Z(F) \subset \mathbb{A}^2$ be an affine plane curve defined over \mathbb{F}_q by an equation $F(X, Y) \in \mathbb{F}_q[X, Y]$. One should remark, that we neither assume that F is

irreducible nor that C is smooth. Let

$$C^* = Z(F) \cap (\mathbb{G}_m \times \mathbb{G}_m) \subset \mathbb{G}_m \times \mathbb{G}_m$$

be the corresponding algebraic subset of the two-dimensional torus.

Let $L \subset \mathbb{F}_q[X, Y]$ be a \mathbb{F}_q -linear subspace of dimension τ . The locus Γ^* we are going to study consists of τ -tuples $(P_1 = (x_1, y_1), \dots, P_\tau = (x_\tau, y_\tau))$, of points on C^* failing to impose independent conditions on L , i.e. there is a polynomial in L vanishing at all the points $P_1 = (x_1, y_1), \dots, P_\tau = (x_\tau, y_\tau)$. If G_1, \dots, G_τ is a basis for L as a vectorspace over \mathbb{F}_q , this amounts to the vanishing of the determinant of the $\tau \times \tau$ -matrix:

$$\begin{vmatrix} G_1(x_1, y_1) & G_1(x_2, y_2) & \dots & G_1(x_\tau, y_\tau) \\ G_2(x_1, y_1) & G_2(x_2, y_2) & \dots & G_2(x_\tau, y_\tau) \\ \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \dots & \cdot \\ G_\tau(x_1, y_1) & G_\tau(x_2, y_2) & \dots & G_\tau(x_\tau, y_\tau) \end{vmatrix}$$

Let $D \in \mathbb{F}_q[X_1, Y_1, \dots, X_\tau, Y_\tau]$ be the polynomial

$$D = \begin{vmatrix} G_1(X_1, Y_1) & G_1(X_2, Y_2) & \dots & G_1(X_\tau, Y_\tau) \\ G_2(X_1, Y_1) & G_2(X_2, Y_2) & \dots & G_2(X_\tau, Y_\tau) \\ \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \dots & \cdot \\ G_\tau(X_1, Y_1) & G_\tau(X_2, Y_2) & \dots & G_\tau(X_\tau, Y_\tau) \end{vmatrix}$$

Let d be the maximum of the degrees $\deg(G_i), i = 1, \dots, \tau$ and let $\tilde{D} \in \mathbb{F}_q[X_1, Y_1, Z_1, \dots, X_\tau, Y_\tau, Z_\tau]$ be the homogeneous polynomial of degree τd obtained as the determinant:

$$\tilde{D} = \begin{vmatrix} Z_1^d G_1\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) & Z_2^d G_1\left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right) & \dots & Z_\tau^d G_1\left(\frac{X_\tau}{Z_\tau}, \frac{Y_\tau}{Z_\tau}\right) \\ Z_1^d G_2\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) & Z_2^d G_2\left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right) & \dots & Z_\tau^d G_2\left(\frac{X_\tau}{Z_\tau}, \frac{Y_\tau}{Z_\tau}\right) \\ \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \dots & \cdot \\ Z_1^d G_\tau\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) & Z_2^d G_\tau\left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right) & \dots & Z_\tau^d G_\tau\left(\frac{X_\tau}{Z_\tau}, \frac{Y_\tau}{Z_\tau}\right) \end{vmatrix} \quad (6)$$

Note that all polynomials in the above matrix are homogeneous of degree d .

Definition 7 *The locus Γ^* of τ -tuples of points failing to impose independent conditions on the functions in L is in the notation above the subvariety of $(C^*)^\tau \subset ((\mathbb{G}_m)^2)^\tau$ defined by D :*

$$\Gamma^* = \{(P_1, \dots, P_\tau) \in (C^*)^\tau \mid D = 0\} \subset ((\mathbb{G}_m)^2)^\tau \quad (7)$$

Theorem 8 *Let $L \subset \mathbb{F}_q[X, Y]$ be a \mathbb{F}_q -linear subspace of dimension τ with basis G_1, \dots, G_τ . Let $\deg(G_i) = d_i, i = 1, \dots, \tau$. Let $(C^*)^\tau \subset ((\mathbb{G}_m)^2)^\tau$ and let Γ^* be defined as in (7). Let \tilde{D} be the determinant (6). Assume that $q - 1$ and τd are coprime. Then*

$$\frac{S((\tilde{C}^*)^\tau, \tilde{D})}{(q - 1)^{(\tau-1)}} = q |\Gamma^*(\mathbb{F}_q)| - |(C^*)^\tau(\mathbb{F}_q)|,$$

where $S((\tilde{C}^*)^\tau, \tilde{D})$ is the exponential sum on $(\tilde{C}^*)^\tau$.

PROOF. Let $\tilde{F}(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ be the homogenized equation. Let

$$\tilde{C}^* = Z(\tilde{F}) \cap (\mathbb{G}_m \times \mathbb{G}_m \times \mathbb{G}_m) \subset \mathbb{G}_m \times \mathbb{G}_m \times \mathbb{G}_m$$

be the corresponding algebraic subset of the torus and let $V \subset (\mathbb{G}_m \times \mathbb{G}_m \times \mathbb{G}_m)^\tau$ be defined by the homogeneous equations $\tilde{F}(X_i, Y_i, Z_i), i = 1, \dots, \tau$. Lemma 6 gives that

$$(q - 1)S((\tilde{C}^*)^\tau, \tilde{D}) = q |V_{\tilde{D}}(\mathbb{F}_q)| - |V(\mathbb{F}_q)|.$$

Finally, use the fact that \tilde{C}^* is a punctured cone over C^* such that $\tilde{C}^*(\mathbb{F}_q)$ is a $(q - 1)$ -fold covering of $C^*(\mathbb{F}_q)$ and consequently $(\tilde{C}^*)^\tau(\mathbb{F}_q)$ is a $(q - 1)^\tau$ -fold covering of $(C^*)^\tau(\mathbb{F}_q)$. Likewise as \tilde{D} is homogeneous, $V_{\tilde{D}}(\mathbb{F}_q)$ is a $(q - 1)^\tau$ -fold covering of $V(\mathbb{F}_q)$.

Remark 9 *Let $\tilde{F}(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ be the homogenized equation and $\tilde{F}_i = \tilde{F}(X_i, Y_i, Z_i), i = 1, \dots, \tau$, then $\tilde{D} + \sum_{i=1}^\tau S_i \tilde{F}_i$ is a function on $(\mathbb{G}_m)^{3\tau} \times \mathbb{A}^\tau$ and there is the following relation for exponential sums, see ([B]):*

$$q^\tau S((\tilde{C}^*)^\tau, \tilde{D}) = S((\mathbb{G}_m)^{3\tau} \times \mathbb{A}^\tau, \tilde{D} + \sum_{i=1}^\tau S_i \tilde{F}_i). \quad (8)$$

The symmetric group Σ_τ acts on $(\mathbb{Z}^3)^\tau$ and $(\mathbb{Z})^\tau$ by permutation of the factors and consequently on $(\mathbb{Z}^3)^\tau \times (\mathbb{Z})^\tau$. The set J of indices for the function $\tilde{D} + \sum_{i=1}^\tau S_i \tilde{F}_i$ is stable under this action. Also Σ_τ acts on the index set via permutation of G_1, \dots, G_τ .

Under the combined action of $\Sigma_\tau \times \Sigma_\tau$ on J , the indices $I \subset J$ of the polynomial

$$Z_1^d G_1\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right) Z_2^d G_1\left(\frac{X_2}{Z_2}, \frac{Y_2}{Z_2}\right) \cdots \cdots Z_\tau^d G_\tau\left(\frac{X_\tau}{Z_\tau}, \frac{Y_\tau}{Z_\tau}\right) + S_1 \tilde{F}(X_1, Y_1, Z_1)$$

is a complete set of representatives for the orbits. The function $\tilde{D} + \sum_{i=1}^\tau S_i \tilde{F}_i$ is therefore nondegenerate if the condition of 3.1 is true for every face of the Newton polygon containing an element of I .

We can also simplify the calculation of $\nu_{S_2}(\tilde{D} + \sum_{i=1}^\tau S_i \tilde{F}_i)$ defined in (5). Let Δ be the Newton polyhedron of $\tilde{D} + \sum_{i=1}^\tau S_i \tilde{F}_i$ and let Δ_j be the convex hull of $(0, \dots, 0)$ and the elements in J having the last j coordinates equal to 0. Let vol_j denote the volume of Δ_j in $\mathbb{R}^{4\tau-j}$. Using the above group action on the J and hence on the Newton polyhedron and its coordinate plane sections, we obtain

$$\nu_{S_2}(\tilde{D} + \sum_{i=1}^\tau S_i \tilde{F}_i) = \sum_{j=0}^\tau (-1)^{|j|} \binom{\tau}{j} (4\tau - j)! \text{vol}_j \quad (9)$$

Theorem 10 In the notation above, let Δ be the Newton polyhedron of $\tilde{D} + \sum_{i=1}^\tau S_i \tilde{F}_i$. Let Δ_j be the convex hull of $(0, \dots, 0)$ and the elements in J having the last j coordinates equal to 0. Let vol_j denote the volume in $\mathbb{R}^{4\tau-j}$ of Δ_j .

Assume that $\tilde{D} + \sum_{i=1}^\tau S_i \tilde{F}_i$ is nondegenerate and assume that $\text{char}(\mathbb{F}_q) = p \in S_\Delta$, as defined in 3.1.

Then

$$\left| \frac{|\Gamma^*(\mathbb{F}_q)|}{|(C^*)^\tau(\mathbb{F}_q)|} - \frac{1}{q} \right| \leq \left(\sum_{j=0}^\tau (-1)^{|j|} \binom{\tau}{j} (4\tau - j)! \text{vol}_j \right) \frac{1}{|(C^*)^\tau(\mathbb{F}_q)|} \left(\frac{q}{q-1} \right)^{\tau-1}.$$

PROOF. Combining Theorem 8, (8) and Theorem 5 we get

$$\begin{aligned} |q |\Gamma^*(\mathbb{F}_q)| - |(C^*)^\tau(\mathbb{F}_q)|| &\leq \frac{\nu_{S_2}(\tilde{D} + \sum_{i=1}^\tau S_i \tilde{F}_i) \sqrt{q}^{3\tau+\tau}}{(q-1)^{(\tau-1)} q^\tau} = \\ &\nu_{S_2}(\tilde{D} + \sum_{i=1}^\tau S_i \tilde{F}_i) \frac{q^\tau}{(q-1)^{(\tau-1)}}. \end{aligned}$$

Using (9) the conclusion follows.

As for the field extension \mathbb{F}_{q^i} , it follows by the same methods that

$$\left| \frac{|\Gamma^*(\mathbb{F}_{q^i})|}{|(C^*)^\tau(\mathbb{F}_{q^i})|} - \frac{1}{q^i} \right| \leq \left(\sum_{j=0}^{\tau} (-1)^{|j|} \binom{\tau}{j} (4\tau - j)! \text{vol}_j \right) \frac{1}{|(C^*)^\tau(\mathbb{F}_{q^i})|} \left(\frac{q^i}{q^i - 1} \right)^{\tau-1}$$

References

- [A-S] Adolphson, Alan and Sperber, Steven, Exponential sums and Newton polyhedra: cohomology and estimates, *Ann. of Math. (2)*, *Annals of Mathematics. Second Series*, 130, 1989, 2, 367–406.
- [B] Bombieri, E., On exponential sums in finite fields. II, *Invent. Math.*, 47, 1978, 1, 29–39.
- [D] Deligne, P., La conjecture de Weil. II, *Inst. Hautes Études Sci. Publ. Math.*, 52, 1980.
- [G-L] Ghorpade, S., Lachaud, G., Étale cohomology, Lefschetz Theorems and the number of points of singular varieties over finite fields. , *Prétirages de l'I.M.L.*, 1999, 45 pp.
- [H-L] Hansen, J.P., Lachaud, G., Lefschets theorems and dependent rational points on curves over finite fields, *Dept. of Mathematics, University of Aarhus, Denmark, PREPRINT SERIES* , 1999, No. 4.
- [JNH] Elbrønd Jensen, H., Refslund Nielsen, R. and Høholdt, Performance Analysis of a Decoding Algorithm for Algebraic-Geometry codes, *IEEE Trans. Inform. Theory*, vol. 45, pp. 1712-1717, July 1999.
- [J] Jouanolou, J.P., Cohomologie de quelques schémas classiques et théorie cohomologique des classes de Chern, *Exp. VII in [SGA5]*, 282-350.
- [K] Katz, Nicholas M., Sommes exponentielles, Course taught at the University of Paris, Orsay, Fall 1979, With a preface by Luc Illusie, Notes written by Gérard Laumon, With an English summary, *Société Mathématique de France, Paris*, 1980, 209.
- [K-L] Katz, Nicholas M. and Laumon, Gérard, Transformation de Fourier et majoration de sommes exponentielles, *Inst. Hautes Études Sci. Publ. Math., Institut des Hautes Études Scientifiques. Publications Mathématiques*, 62, 1985, 361–418.
- [La] Lachaud, Gilles, Number of points of plane sections and linear codes defined on algebraic varieties, *Arithmetic, geometry and coding theory (Luminy, 1993)*, 77–104, de Gruyter, Berlin, 1996.

- [M] Milne, James S., *Étale cohomology*, Princeton University Press, Princeton, N.J., 1980, xiii+323.
- [Sh-Sk] Shparlinski I. E. and Skorobogatov A. N., Exponential sums and rational points on complete intersections, *Mathematika* 37 (1990), 201-208.
- [Sk] Skorobogatov A. N., Exponential sums, the geometry of hyperplane sections, and some diophantine problems, *Israel J. Math.* 80 (1992), 359-379.