UNIVERSITY OF AARHUS
DEPARTMENT OF MATHEMATICS

ISSN: 1397-4076

LEFSCHETZ THEOREMS AND DEPENDENT RATIONAL POINTS ON CURVES OVER FINITE FIELDS

By Johan P. Hansen and Gilles Lachaud

Preprint Series No.: 4 March 1999

Ny Munkegade, Bldg. 530
8000 Aarhus C, Denmark
http://www.imf.au.dk
institut@imf.au.dk

LEFSCHETZ THEOREMS AND DEPENDENT RATIONAL POINTS ON CURVES OVER FINITE FIELDS.

JOHAN P. HANSEN AND GILLES LACHAUD

Abstract. For a smooth curve C over a finite field $\mathbb{F}_q$, we prove that the probability that a randomly chosen set of τ rational points impose dependent conditions on a given linear system of dimension τ is asymptotically equal to $\frac{1}{q}$.

The proof involves a geometric construction and a Lefschetz theorem for quasi-projective varieties.

The result has applications in the assessment of the performance of decoding algorithms for algebraic geometry codes.

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.

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

and let $\Gamma \subset X$ 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

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

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. Then we prove that

Document version: March 24, 1999.

1991 *Mathematics Subject Classification.* 14F20, 14G10, 14G15, 14H25, (94B27), (94B35).

Key words and phrases. Lefschetz theorem, Points failing to impose independent conditions, (Error-correcting Codes, decoding).

This work was done while the first author visited: Équipe "Arithemetique et Théorie de l'Information" Institut de Mathématique de Luminy. The first author would very much like to express his gratitude to the Équipe and to the Institut de Mathématique de Luminy.

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

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

The bounding term $c\,(q^j)^{\frac{\tau+1}{2}}$ can not in general be replaced by a smaller power of q^j, as the following example show.

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 is 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. Vi now have for all uneven j, that

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

A result of the above type has applications in the assessment of the performance of decoding algorithms for algebraic geometry codes according to [JNH].

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

Proof. Let $(a_{i,1} : \ldots : a_{i,\tau})$ be homogenous coordinates on the i'th copy of $\mathbb{P}^{\tau-1}$ in $\mathbb{P}^{\tau-1} \times \ldots \times \mathbb{P}^{\tau-1}$ and let $V \subset \mathbb{P}^{\tau-1} \times \ldots \times \mathbb{P}^{\tau-1}$ 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

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

the morphism defined by

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

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

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

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

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

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

and we note the important fact that

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

It follows that $X\backslash\Gamma$ 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 $(P_1, \ldots, P_\tau) \in \Gamma$ is a singular point on Γ, this implies that H (and thereby V) do not intersect X transversally at $(P_1, \ldots, P_\tau)$.

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

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

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

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

As the intersection between X and V isn't transversal at $(P_1, \ldots, P_\tau)$, the intersection between X and $P_1 \times \ldots P_{j-1} \times L \times P_{j+1} \times \ldots \times P_\tau$ can't be either, consequently L is a tangent hyperplane to the curve C at P_j. This is true for all $P_1, \ldots, P_\tau$, i.e. , there exists a rational functions in $L(D)$ vanishing to at least second order at $P_1, \ldots, P_\tau$, therefore $l(D - (2P_1 + \ldots 2P_\tau)) > 0$, 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 $\mathrm{H}^i(X,\mathcal{F})$ (resp. $\mathrm{H}^i_c(X,\mathcal{F})$) denote the étale l-adic chomology groups (resp. the étale l-adic chomology groups with compact support), see [M].

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

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

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 gives 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 $X\backslash Y$ is affine. Then there are isomorphisms:*

$$\mathrm{H}^{i-2}_c(Y,\mathbb{Q}_l(-1)) \to \mathrm{H}^i_c(X,\mathbb{Q}_l)$$

for $i \geq n+2$.

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

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

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

We are ready to prove Theorem 1.

Proof. The ground field is the finite field $\mathbb{F}_q$ and $\mathrm{H}_c^i(X, \mathbb{O}_l)$ 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 ètale cohomology spaces.

We have accordingly

$$|X(\mathbb{F}_q)| = \sum_{i=0}^{2\tau} (-1)^i \operatorname{Tr}(\mathbf{Frob} \mid \mathrm{H}_c^i(X, \mathbb{Q}_l)) \tag{3}$$

$$q\,|\mathbf{\Gamma}(\mathbb{F}_q)| = q \sum_{i=0}^{2\tau-2} (-1)^i \operatorname{Tr}(\mathbf{Frob} \mid \mathrm{H}_c^i(\mathbf{\Gamma}, \mathbb{Q}_l)) \tag{4}$$

As for the high dimensions, we obtain from Lemma 4 applied to X and $\mathbf{\Gamma}$, that

$$q \sum_{i=\tau}^{2\tau-2} (-1)^i \operatorname{Tr}(\mathbf{Frob} \mid \mathrm{H}_c^i(\mathbf{\Gamma}, \mathbb{Q}_l)) = \sum_{i=\tau}^{2\tau-2} (-1)^i \operatorname{Tr}(\mathbf{Frob} \mid \mathrm{H}_c^i(\mathbf{\Gamma}, \mathbb{Q}_l(-1))) =$$
$$\sum_{i=\tau+2}^{2\tau} (-1)^i \operatorname{Tr}(\mathbf{Frob} \mid \mathrm{H}_c^i(X, \mathbb{Q}_l))$$

Combining this with (3) and (4) gives:

$$|X(\mathbb{F}_q)| - q\,|\mathbf{\Gamma}(\mathbb{F}_q)| =$$
$$\sum_{i=0}^{\tau+1} (-1)^i \operatorname{Tr}(\mathbf{Frob} \mid \mathrm{H}_c^i(X, \mathbb{Q}_l)) - q \sum_{i=0}^{\tau-1} (-1)^i \operatorname{Tr}(\mathbf{Frob} \mid \mathrm{H}_c^i(\mathbf{\Gamma}, \mathbb{Q}_l))$$

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 (1) 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 $q^{\frac{\tau+1}{2}}$. □

References

[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.

[JNH] Elbrønd Jensen, H., Refslund Nielsen, R. and Høholdt, Performance analysis of a decoding algorithm for algebraic geometry codes, Preprint, Dept. of Math., Technical Univ. of Denmark, 1998

[J] Jouanolou, J.P., Cohomologie de quelques schémas classiques et théorie cohomologique des classes de Chern, Exp. VII in [SGA5], 282-350

[M] Milne, James S., Étale cohomology, Princeton University Press, Princeton, N.J., 1980, xiii+323,

(JPH) Matematisk Institut, Ny Munkegade, 8000 Aarhus C, Denmark

Current address: Institut de Mathématique de Luminy, 163 avenue de Luminy, Case 907, 13288 Marseille CEDEX 9 , FRANCE

E-mail address, JPH: `matjph@imf.au.dk`

(GL) Institut de Mathématique de Luminy, 163 avenue de Luminy, Case 907, 13288 Marseille CEDEX 9 , FRANCE

E-mail address, GL: `lachaud@iml.univ-mars.fr`