Bull. Korean Math. Soc. **41** (2004), No. 3, pp. 451–456

# DISTRIBUTION OF VALUES OF FUNCTIONS OVER FINITE FIELDS

HI-JOON CHAE

ABSTRACT. Given a function on a scheme over a finite field, we can count the number of rational points of the scheme having the same values. We show that if the function, viewed as a morphism to the affine line, is proper and its higher direct image sheaves are tamely ramified at the infinity then the values are uniformly distributed up to some degree.

## 1. Introduction

Let $X_0$ be a scheme of finite type over a finite field $\mathbf{F}_q$ of order $q$ and let $X = X_0 \otimes \mathbf{F}$ where $\mathbf{F}$ is an algebraic closure of $\mathbf{F}_q$. Let $f$ be a function on $X_0$, in other words a morphism $f : X_0 \to \mathbf{A}^1_{\mathbf{F}_q}$. For each extension $\mathbf{F}_{q^n}$ of $\mathbf{F}_q$ in $\mathbf{F}$, we have $f_n : X(\mathbf{F}_{q^n}) \to \mathbf{A}^1(\mathbf{F}_{q^n})$. Professor Dae San Kim raised the following question: when are the values of the function $f$ distributed uniformly on $X$? In other words, when $|f_n^{-1}(y)| \approx |X(\mathbf{F}_{q^n})|/q^n$ for each $y \in \mathbf{F}_{q^n}$ with $n$ sufficiently large?

With the interpretation of exponential sums in terms of $\ell$-adic cohomology and the proper base change theorem, the problem reduces to the study of higher direct image sheaves with compact support $\mathrm{R}^i f_! \overline{\mathbf{Q}}_\ell$ on $\mathbf{A}^1_{\mathbf{F}_q}$. In this perspective, if (some of) $\mathrm{R}^i f_! \overline{\mathbf{Q}}_\ell$'s are *geometrically constant*, i.e. if their inverse images to $\mathbf{A}^1_{\mathbf{F}}$ are constant, then we can deduce the equidistribution of values of $f$ up to some degree.

When $f$ is proper, it follows from the theory of vanishing cycles that $\mathrm{R}^i f_! \overline{\mathbf{Q}}_\ell$'s of high degree are lisse. If they are tamely ramified at the infinity (of $\mathbf{A}^1_{\mathbf{F}_q}$), then they are constant on $\mathbf{A}^1_{\mathbf{F}}$. The assumption of

Received March 31, 2004.

2000 Mathematics Subject Classification: 11T23, 11G25, 14G15.

Key words and phrases: distribution, values of functions, finite fields.

This work was supported by grant No.R01-2002-000-00083-0(2002) from the Basic Research Program of the Korea Science and Engineering Foundation.

properness can be replaced by the condition of regularity at the infinity (of $X_0$). In the last section, we give some remarks on the general case.

The author would like to thank Professor Dae San Kim for helpful discussions.

## 2. Counting rational points and weights

Throughout the paper, we fix a prime number $\ell$. For a prime number $p \neq \ell$, $\mathbf{F}_p$ denotes a finite field with $p$ elements and $\mathbf{F}$ its algebraic closure. For a power $q$ of $p$, $\mathbf{F}_q$ denotes the subfield of $\mathbf{F}$ of order $q$. By a sheaf, unless otherwise stated, we always mean a $\overline{\mathbf{Q}}_\ell$-sheaf.

Following the usual convention, objects defined over $\mathbf{F}_q$ will be denoted with subscription 0, while objects obtained from them by extending $\mathbf{F}_q$ to $\mathbf{F}$ will be denoted without the subscription. For example, if $X_0$ is a scheme of finite type over $\mathbf{F}_q$ and $\mathfrak{F}_0$ is a sheaf on it, then $\mathfrak{F}$ is the inverse image of $\mathfrak{F}_0$ on $X = X_0 \otimes_{\mathbf{F}_q} \mathbf{F}$. We have the *Frobenius morphism* $F : X_0 \to X_0$ and an isomorphism $F^* : F^*\mathfrak{F}_0 \xrightarrow{\sim} \mathfrak{F}_0$. Extending scalars, we have $F : X \to X$ and for each $n$ the fixed point set $X^{F^n}$ of $X$ under $F^n$ is $X(\mathbf{F}_{q^n})$. The pair $(F, F^*)$ induces endomorphisms $F^*$ of compact support cohomology groups $H_c^i(X, \mathfrak{F})$ and for each closed point $x$ of $X_0$ the endomorphism $F_x$ of the stalk $\mathfrak{F}_{\bar{x}}$ where $\bar{x}$ is any geometric point localized at $x$. The sums of traces of Frobenius morphisms on stalks are related to those of Frobenius morphisms on cohomology groups as follows.

THEOREM 1 (Grothendieck-Lefschetz trace formula). *Let $X_0$ be a scheme of finite type over $\mathbf{F}_q$ and $\mathfrak{F}_0$ a constructible sheaf on it. For each positive integer $n$ we have*

$$\sum_{x \in X(\mathbf{F}_{q^n})} tr((F^n)^*, \mathfrak{F}_x) = \sum_i (-1)^i tr((F^*)^n, H_c^i(X, \mathfrak{F})).$$

In particular, the number of $\mathbf{F}_{q^n}$ rational points of $X$ is given by

$$|X(\mathbf{F}_{q^n})| = \sum_i (-1)^i \mathrm{tr}((F^*)^n, H_c^i(X, \overline{\mathbf{Q}}_\ell)).$$

This formula combined with the following theory of weights gives sharp estimates of exponential sums. $\mathfrak{F}_0$ is said to be *punctually pure* of weight $w$ if for each closed point $x$ of $X_0$, all the eigenvalues of $F_x$ acting on $\mathfrak{F}_{\bar{x}}$ are of complex absolute value $N(x)^{w/2}$ for any embedding $\overline{\mathbf{Q}}_\ell \to \mathbf{C}$, where $N(x) = q^{\deg(x)}$ is the order of the residue field of $x$. $\mathfrak{F}_0$

is said to be *mixed* (of weight $\leq w$) if it admits a finite filtration whose quotients are punctually pure (of weight $\leq w$). One of the main results of [1] is the following.

THEOREM 2 ([1], Théorème 3.3.1). *Let $f : X_0 \to S_0$ be a morphism of schemes of finite type over $\mathbf{F}_q$ and $\mathfrak{F}_0$ a mixed sheaf of weight $\leq n$ on $X_0$. Then for each $i$, the sheaf $R^i f_! \mathfrak{F}_0$ on $S_0$ is mixed of weight $\leq n+i$.*

All the definitions and results above can be generalized to objects of $D_c^b(X_0, \overline{\mathbf{Q}}_\ell)$ in place of a single sheaf.

## 3. Rational points of fibers

Let $X_0$ be a normal, geometrically connected scheme of finite type over $\mathbf{F}_q$ and $f$ a function on it, in other words, $f : X_0 \to \mathbf{A}^1_{\mathbf{F}_q}$ is a morphism. For each $y \in \mathbf{F}_q$ we consider the number of rational points of the fiber over $y$, $|f^{-1}(y)(\mathbf{F}_q)| = |\{x \in X(\mathbf{F}_q) | f(x) = y\}|$. We are interested in how these numbers vary over $y \in \mathbf{F}_q$. By the Grothendieck-Lefschetz fixed point formula above, we have

$$|f^{-1}(y)(\mathbf{F}_{q^n})| = \sum_i (-1)^i \mathrm{tr}((F^*)^n, H_c^i(f^{-1}(y), \overline{\mathbf{Q}}_\ell)).$$

On the other hand, by the proper base change theorem, the compact support cohomology group $H_c^i(f^{-1}(y), \overline{\mathbf{Q}}_\ell)$ of the fiber over $y$ is isomorphic to the stalk at $y$ of the higher direct image with compact support $\mathrm{R}^i f_! \overline{\mathbf{Q}}_\ell$ and this isomorphism is compatible with Frobenius morphisms. So we should consider sheaves $\mathrm{R}^i f_! \overline{\mathbf{Q}}_\ell$ on $\mathbf{A}^1_{\mathbf{F}_q}$. The sheaves $\mathrm{R}^i f_! \overline{\mathbf{Q}}_\ell$ are not necessarily lisse even when $X$ and $f$ are smooth. In general, they are only constructible, hence are lisse outside a finite number of points in $\mathbf{A}^1_{\mathbf{F}_q}$. When we impose the properness and the tame ramification at the infinity we get the following.

THEOREM 3. *Let $X_0$ be a normal geometrically connected scheme of finite type over $\mathbf{F}_q$ and $f : X_0 \to \mathbf{A}^1_{\mathbf{F}_q}$ a proper and flat morphism. Let $d$ be the dimension of the generic fiber. Suppose that each $R^i f_! \overline{\mathbf{Q}}_\ell$ is tamely ramified at the infinity.*

(1) *If $f$ is smooth, then each $R^i f_! \overline{\mathbf{Q}}_\ell$ is geometrically constant and for each $y \in \mathbf{A}^1(\mathbf{F}_{q^n})$, we have $|f^{-1}(y)(\mathbf{F}_{q^n})| = |X(\mathbf{F}_{q^n})|/q^n$.*

(2) *Let $\Sigma$ be the locus of non-smooth points of $f$ and $k$ be the maximum of dimensions of $\Sigma_s$ for $s \in \mathbf{A}^1$. For $i > d+k+1$, the sheaf $R^i f_! \overline{\mathbf{Q}}_\ell$ is geometrically constant. For each $y \in \mathbf{A}^1(\mathbf{F}_{q^n})$, we have $|f^{-1}(y)(\mathbf{F}_{q^n})| = |X(\mathbf{F}_{q^n})|/q^n + O(q^{n(d+k+1)/2})$.*

*Proof.* We follow the line of the proof of [3, (3.1)] Let $\bar{s}$ be a geometric point lying over a closed point $s$ of $\mathbf{A}^1_{\mathbf{F}_q}$ and let $\bar{\eta}$ be a geometric generic point of the henselization of $\mathbf{A}^1_{\mathbf{F}_q}$ at $s$. Since $f$ is proper, we have a long exact sequence [2, (2.1.8.9)]

$$\cdots \to \mathrm{H}^i(X_{\bar{s}}, \overline{\mathbf{Q}}_\ell) \to \mathrm{H}^i(X_{\bar{\eta}}, \overline{\mathbf{Q}}_\ell) \to \mathrm{H}^i(X_{\bar{s}}, \mathrm{R}\Phi_{\bar{\eta}}(\overline{\mathbf{Q}}_\ell)) \to \cdots$$

where $\mathrm{R}\Phi(\overline{\mathbf{Q}}_\ell)$ denotes the complex of vanishing cycles.

(1) If $f$ is smooth, then $\mathrm{R}\Phi(\overline{\mathbf{Q}}_\ell) = 0$ [2, (2.1.5)] hence from the above exact sequence we can see that sheaves $\mathrm{R}^i f_!(\overline{\mathbf{Q}}_\ell)$ on $\mathbf{A}^1_{\mathbf{F}_q}$ are lisse. Since they are tamely ramified at the infinity, their inverse images to $\mathbf{A}^1_{\mathbf{F}}$ is constant. This follows from the fact that the fundamental group of $\mathbf{A}^1_{\mathbf{F}}$ has no nontrivial finite quotient of order prime to $p = \mathrm{char}(\mathbf{F})$, which is a part of the Abhyankar's conjecture for the affine line [7]. If $\mathfrak{F}_0$ is a lisse sheaf on a scheme $X_0$ over $\mathbf{F}_q$ whose inverse image to $X$ is constant, then the action of the arithmetic fundamental group $\pi_1(X_0, \bar{x})$ on the stalk $\mathfrak{F}_{\bar{x}}$ at a geometric point $\bar{x}$ factors through $\mathrm{Gal}(\mathbf{F}/\mathbf{F}_q)$ in the long exact sequence

$$0 \to \pi_1(X, \bar{x}) \to \pi_1(X_0, \bar{x}) \to \mathrm{Gal}(\mathbf{F}/\mathbf{F}_q) \to 0$$

since the geometric fundamental group $\pi_1(X, \bar{x})$ acts trivially. In other words, for any closed point $y$ of $X_0$ the eigenvalues of the Frobenius endomorphism $F_y$ acting on $\mathfrak{F}_{\bar{y}}$ depends only on the degree of $y$. Applying this to $\mathrm{R}^i f_!(\overline{\mathbf{Q}}_\ell)$ on $\mathbf{A}^1_{\mathbf{F}_q}$ we get the second result of (1). Really, for each $y \in \mathbf{A}^1(\mathbf{F}_{q^n})$, $\sum_i (-1)^i \mathrm{tr}((F^n)^*, \mathrm{R}^i f_!(\overline{\mathbf{Q}}_\ell)_y) = |f^{-1}(y)(\mathbf{F}_{q^n})|$ is independent of $y$, hence is equal to $|X(\mathbf{F}_{q^n})|/q^n$.

(2) The first statement is just [4, (4.3)]. Since the proof, which must be obvious to experts, is omitted there, we sketch it. By [4, (4.2)] the dimension of the support of $\mathrm{R}^i\Phi(\overline{\mathbf{Q}}_\ell)$ on $X_{\bar{s}}$ is less than or equal to $d - i$. It follows that in the spectral sequence $\mathrm{H}^p(X_{\bar{s}}, \mathrm{R}^q\Phi_{\bar{\eta}}\overline{\mathbf{Q}}_\ell) \Rightarrow \mathrm{H}^{p+q}(X_{\bar{s}}, \mathrm{R}\Phi_{\bar{\eta}}\overline{\mathbf{Q}}_\ell)$, the $(p, q)$ term vanishes unless $p+2q \leq 2d$ and $p \leq 2k$. Hence $\mathrm{H}^i(X_{\bar{s}}, \mathrm{R}\Phi_{\bar{\eta}}\overline{\mathbf{Q}}_\ell) = 0$ for $i > d + k$ and $\mathrm{H}^i(X_{\bar{s}}, \overline{\mathbf{Q}}_\ell) \to \mathrm{H}^i(X_{\bar{\eta}}, \overline{\mathbf{Q}}_\ell)$ in the above long exact sequence is an isomorphism for $i > d + k + 1$. By the same arguments as above, $\mathrm{R}^i f_!(\overline{\mathbf{Q}}_\ell)$ is geometrically constant for

$i > d+k+1$. Let $y \in \mathbf{F}_{q^n}$, then we have

$$\begin{aligned} |X(\mathbf{F}_{q^n})| &= \sum_{z\in\mathbf{F}_{q^n}} |f^{-1}(z)(\mathbf{F}_{q^n})| \\ &= \sum_{z\in\mathbf{F}_{q^n}} \sum_{i} (-1)^i \mathrm{tr}((F^n)^*, (\mathrm{R}^i f_! \overline{\mathbf{Q}}_\ell)_z) \\ &= q^n \sum_{i>d+k+1} (-1)^i \mathrm{tr}((F^n)^*, (\mathrm{R}^i f_! \overline{\mathbf{Q}}_\ell)_y) \\ &\quad + \sum_{z} \sum_{i\le d+k+1} (-1)^i \mathrm{tr}((F^n)^*, (\mathrm{R}^i f_! \overline{\mathbf{Q}}_\ell)_z). \end{aligned}$$

Since $\mathrm{R}^i f_! \overline{\mathbf{Q}}_\ell$ is mixed of weight $\le i$, the second result of (2) follows. □

## 4. Remarks

(1) Without the assumption of the properness of $f$, the above arguments still can be applied in some cases. For example, if $f : X_0 \to \mathbf{A}^1_{\mathbf{F}_q}$ factors through $X_0 \hookrightarrow \overline{X}_0 \to \mathbf{A}^1_{\mathbf{F}_q}$ where $\overline{X}_0 \to \mathbf{A}^1_{\mathbf{F}_q}$ is proper and flat, and the complement of $X_0$ in $\overline{X}_0$ is a relative divisor with normal crossings, then we can apply the same arguments as in the proof of the above theorem [2, (2.1.9)].

(2) In general, we can not expect a uniform distribution of values of function. More precisely, as explained in the last section, the sheaf $\mathfrak{F}_0 = \mathrm{R}^i f_! \overline{\mathbf{Q}}_\ell$ is lisse on an open dense subset $U_0 \subset \mathbf{A}^1_{\mathbf{F}_q}$.

A lisse sheaf $\mathfrak{F}_0$ on a smooth curve $U_0$ over $\mathbf{F}_q$ defines a representation of the arithmetic fundamental group $\pi_1(U_0, \bar{x})$ on the stalk $\mathfrak{F}_{\bar{x}}$ at a geometric point $\bar{x}$, in other words, a homomorphism $\pi_1(U_0, \bar{x}) \to \mathrm{GL}(\mathfrak{F}_{\bar{x}})$. The Zariski closure $G^0$ of the image of $\pi_1(U)$ in $\mathrm{GL}_{\overline{\mathbf{Q}}_\ell}$ is called the *geometric monodromy group* of $\mathfrak{F}_0$. So $\mathfrak{F}_0$ is geometrically constant if and only if $G^0 = \{e\}$. Let $G$ be the extension by $G^0$ of the subgroup $\mathbf{Z}$ of $\mathrm{Gal}(\mathbf{F}/\mathbf{F}_q)$ generated by the Frobenius element as in [1, (1.3.7)]. For each closed point $x$ of $U_0$, the Frobenius morphism $F_x$ defines a conjugacy class in $G$.

If $\mathfrak{F}_0$ is semisimple, or more generally if geometrically semisimple, then the connected component of the geometric monodromy group is semisimple [1, (1.3.9)]. And, roughly speaking, the Frobenius elements $F_x$ are "equidistributed" in the space $G^\natural_{\mathbf{R}}$ of conjugacy classes in a maximal compact (modulo center) subgroup $G_{\mathbf{R}}$ of $G_{\mathbf{C}} = G \otimes_{\overline{\mathbf{Q}}_\ell} \mathbf{C}$ [1, (3.5.3)].

If $\mathfrak{F}_0$ is lisse and mixed, as in our case, then it admits an increasing filtration by lisse sheaves whose successive quotients are punctually pure. Moreover, lisse and punctually pure sheaf on a normal scheme is geometrically semisimple [1, (3.4.1)]. Hence we can apply the equidistribution theorem to these components of the filtration.

Now consider our case of $\mathfrak{F}_0 = \mathrm{R}^i f_! \overline{\mathbf{Q}}_\ell$ which is mixed and lisse on some open $U_0 \subset \mathbf{A}^1_{\mathbf{F}_q}$. As above it admits an increasing filtration by lisse sheaves whose quotients are punctually pure. If all these components are geometrically constant, then we can deduce the equidistribution of values of $f$ on $U$ as in the last theorem.

(3) Let $R$ be a finitely generated subring of $\mathbf{C}$ and $X$ be a scheme of finite type over $R$. If $f : X \to \mathbf{A}^1_R$ is a morphism over $R$, we may consider its "reduction" $f_\phi : X_\phi \to \mathbf{A}^1_{R_\phi}$ for each homomorphism $\phi : R \to k$ onto a finite field $k$. Then for almost all $\phi$, the sheaves $\mathrm{R}^i(f_\phi)_! \overline{\mathbf{Q}}_\ell$ are tamely ramified at the infinity. More precisely, there exists a positive integer $N$ and a divisor $D$ of $\mathbf{A}^1_{R[1/N]}$ which is finite and etale over $R[1/N]$ such that for any lisse sheaf $\mathfrak{F}$ on $X$, each $\mathrm{R}^i f_! \mathfrak{F}$ are lisse on $\mathbf{A}^1_{R[1/N]} - D$ and $D$ [6, (3.1.2)]. They are tamely ramified along $D \cup \{\infty\}$ [5, (4.7.1)]. Hence if $f$ is proper, then for "reduction" of $f$ module $\phi$ not dividing $N\ell$, we can apply the last theorem.

## References


[1] P. Deligne, *La conjecture de Weil, II*, Publ. Math. IHES **52** (1980), 137–252.

[2] ———, *Le formalisme des cycles évanescents*, in Groupes de Monodromie en Géométrie Algébrique, Séminaire de Géométrie Algébrique 7 II, by P. Deligne and N. Katz, Lecture Notes in Math. **340** (1973), 82–115.

[3] J. Denef and F. Loeser, *Weights of exponential sums, intersection cohomology and Newton polyhedra*, Invent. Math. **106** (1991), 275–294.

[4] A. Grothendieck, *Exposé I*, in Groupes de Monodromie en Géométrie Algébrique, Séminaire de Géométrie Algébrique 7 I, by A. Grothendieck, M. Raynaud and D. S. Rim, Lecture Notes in Math. **288** (1972), 1–24.

[5] N. Katz, *Sommes exponentielles*, Astérisque **79** (1980).

[6] N. Katz and G. Laumon, *Transformation de Fourier et majoration de sommes exponentielles*, Publ. Math. IHES **62** (1985), 145–202.

[7] M. Raynaud, *Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar*, Invent. Math. **116** (1994), 425–462.



Department of Mathematics Education, Hongik University, Seoul 121-791, Korea

*E-mail*: hchae@math.hongik.ac.kr