An exponential sum and higher-codimensional subvarieties of projective spaces over finite fields

Kazuaki Miyatani and Makoto Sano

Abstract. A general method to express in terms of Gauss sums the number of rational points of general subschemes of projective schemes over finite fields is applied to the image of the triple embedding $\mathbf{P}^1 \hookrightarrow \mathbf{P}^3$. As a consequence, we obtain a non-trivial description of the value of a Kloosterman-sum-like exponential sum.

Introduction

Based on a calculation concerning the diagonal hypersurfaces and Jacobi sums, André Weil [12] observed that the number of rational points of algebraic varieties over finite fields is a highly geometric information. His celebrated Weil conjecture is eventually proved by Pierre Deligne [1] with Grothendieck's theory of étale cohomology.

Another, and the first, proof by Bernard Dwork [3] of the rationality of zeta function, a part of Weil conjecture, more directly concerns exponential sums. In the very beginning of his proof, he reduces the rationality of the zeta function of algebraic varieties to that of hypersurfaces of $(\mathbf{G}_{\mathrm{m}})^n$, and writes the number of rational points of the hypersurface by using exponential sums.

Besides such general theories, expressing the number of rational points using exponential sums has proved to be effective also in studying concrete projective hypersurfaces; the study of Dwork families, for example by Neal Koblitz [9], is one of the most outstanding success of this strategy. It seems therefore natural to expect the efficacy of this tactic in studying projective varieties of higher codimension. This point of view, however, does not seem to be taken note of enough in the study of concrete algebraic varieties of higher codimension.

In the former half of this article, we explain the general method for obtaining a formula for the number of rational points of projective varieties in terms of Gauss sums. Then, in the latter half, we apply the method to get an expression for the number of rational points of the image V of the

triple embedding $\mathbf{P}^1 \hookrightarrow \mathbf{P}^3$. Equating the result with the obvious equation $\#V(\mathbf{F}_q) = q + 1$, we get a non-trivial equation on an exponential sum (Corollary 1);

$$\sum_{t_1, t_2, t_3 \in \mathbf{F}_q^\times} \theta(t_1 + t_2 + t_3 - t_1^2 t_2^{-2} t_3 - t_1^2 t_2^{-3} t_3^2 - t_1 t_2^{-2} t_3^2) = 2q^2 - 3q - 1,$$

where θ denotes a non-trivial character on $\mathbf{F}_q$. This result is also viewed as a description of the Frobenius trace on a pull-back of an Artin–Schreier sheaf by an appropriate morphism $(\mathbf{G}_m)^3 \to \mathbf{A}^1$. In the last section, we work on another subscheme of projective spaces, the image of the Segre embedding $\mathbf{P}^1 \times \mathbf{P}^2 \hookrightarrow \mathbf{P}^5$, to see that the character sum L above again appears in this calculation.

The authors expect that the content of this article can help the future study of the following two objects. The first is the zeta function of concrete varieties; the method described in this article is expected to make it possible to compute zeta function of possibly non-rational varieties of higher codimension in projective spaces. The second is Kloosterman-sum-like exponential sums; an explicit calculation of them may be possible by reducing the problem to finding a variety the number of whose rational points is expressed by using the exponential sum but is already known in some other methods.

Conventions and notations

Throughout this article, we fix a prime number p, a power q of p, and a prime number l different from p.

The n-dimensional projective space $\mathbf{P}_{\mathbf{F}_q}^n$ (resp. affine space $\mathbf{A}_{\mathbf{F}_q}^n$) over $\mathbf{F}_q$ is simply denoted by $\mathbf{P}^n$ (resp. $\mathbf{A}^n$), and similarly, the torus $\mathbf{G}_{m,\mathbf{F}_q} = \operatorname{Spec} \mathbf{F}_q[t, t^{-1}]$ is denoted by $\mathbf{G}_m$. Unless otherwise stated, the term "rational point" refers to "$\mathbf{F}_q$-rational point".

The group of multiplicative characters $\mathbf{F}_q^\times \to \overline{\mathbf{Q}}_l^\times$ is denoted by $\widehat{\mathbf{F}_q^\times}$. The trivial character is denoted by ε. Each character $\chi \in \widehat{\mathbf{F}_q^\times}$, possibly trivial one, is also regarded as a function on $\mathbf{F}_q$ by putting $\chi(0) = 0$.

Finally, *we fix a non-trivial additive character θ: $\mathbf{F}_q \to \overline{\mathbf{Q}}_l^\times$ throughout this article.*

1. Preliminaries on Gauss sum

In this section, we briefly recall the definition and some basic properties of Gauss sums used in this article. Note that we have fixed a non-trivial additive character θ: $\mathbf{F}_q \to \overline{\mathbf{Q}}_l^\times$.

DEFINITION 1. For a character $\chi \in \widehat{\mathbf{F}_q^\times}$, the Gauss sum of χ is defined to be

$$G_\theta(\chi) := \sum_{x \in \mathbf{F}_q^\times} \theta(x)\chi(x).$$

Although the Gauss sum depends on the choice of θ, we usually denote it simply by $G(\chi)$.

The following three equations on characters are fundamental in doing calculations involving Gauss sums.

LEMMA 1. *The following equations hold.*
(i) *For each $x \in \mathbf{F}_q$,*

$$\sum_{w \in \mathbf{F}_q} \theta(wx) = \begin{cases} 0 & \text{if } x \neq 0, \\ q & \text{if } x = 0. \end{cases}$$

(ii) *For each $\chi \in \widehat{\mathbf{F}_q^\times}$,*

$$\sum_{x \in \mathbf{F}_q^\times} \chi(x) = \begin{cases} 0 & \text{if } \chi \neq \varepsilon, \\ q - 1 & \text{if } \chi = \varepsilon. \end{cases}$$

(iii) *For each $x \in \mathbf{F}_q^\times$,*

$$\sum_{\chi \in \widehat{\mathbf{F}_q^\times}} \chi(x) = \begin{cases} 0 & \text{if } x \neq 1, \\ q - 1 & \text{if } x = 1. \end{cases}$$

Now, we list two basic facts on Gauss sums.

PROPOSITION 1. *For each character $\chi \in \widehat{\mathbf{F}_q^\times}$,*

$$G(\chi)G(\chi^{-1}) = \begin{cases} q\chi(-1) & \text{if } \chi \neq \varepsilon, \\ 1 & \text{if } \chi = \varepsilon. \end{cases}$$

PROPOSITION 2. *For each $x \in \mathbf{F}_q^\times$,*

$$\theta(x) = \frac{1}{q} \sum_{\chi \in \widehat{\mathbf{F}_q^\times}} G(\chi^{-1})\chi(x).$$

The detailed proofs for these propositions are omitted; they are straightforward by using Lemma 1 (i) for Proposition 1, and by using Lemma 1 (ii) for Proposition 2.

2. Computing the number of rational points—general strategy

In this section, we describe, in a general setting, a strategy to express the number of rational points of subschemes of projective spaces over $\mathbf{F}_q$ in terms of Gauss sums. The first crucial point is the following reduction process to hypersurfaces; this process is taken in the proof [3, Theorem 1] of rationality of zeta functions, and is now also used in algorithmic theory of zeta functions [11, 3].

OBSERVATION 1. *We obtain a formula for the number of rational points of a closed subscheme of a projective space if we obtain a formula for the number of rational points of some appropriate hypersurfaces.*

In fact, let V be a projective variety of which we want a formula for the number of rational points. Take a closed immersion of V in a projective space $\mathbf{P}^n$, and let the image be defined by m homogeneous polynomials $f_1, \ldots, f_m$. For each choice of integers $1 \le i_1 < \cdots < i_r \le m$, we set

$$N_{i_1,\ldots,i_r} := \#\{x \in \mathbf{P}^n(\mathbf{F}_q) \mid \exists j \in \{i_1, \ldots, i_r\}, f_j(x) = 0\}.$$

Then, since

$$\#V(\mathbf{F}_q) = \sum_{r=1}^{m} \sum_{1 \le i_1 < \cdots < i_r \le m} (-1)^{r+1} N_{i_1,\ldots,i_r},$$

it suffices to obtain a formula for each $N_{i_1,\ldots,i_r}$, which is exactly the number of rational points of the hypersurface defined by the product $f_{i_1} f_{i_2} \ldots f_{i_r}$.

REMARK 1. A formula for rational points of not necessarily closed subschemes of projective spaces is also obtained because such a subscheme is the difference of two closed subschemes.

For obtaining a formula for the number of rational points of a hypersurface of $\mathbf{P}^n$, it suffices to count the number of rational points of the hypersurface of $\mathbf{A}^{n+1}$ defined by the same polynomial. Moreover, the problem reduces to obtaining a formula for

$$\#\{(x_1, \ldots, x_{n+1}) \in (\mathbf{G}_{\mathrm{m}})^{n+1} \mid [x_1 : \cdots : x_{n+1}] \in V(\mathbf{F}_q)\}$$

because the locus with at least one coordinates being zero is covered by hypersurfaces of lower-dimensional affine spaces.

REMARK 2. When dealing with a specific projective variety $V \subset \mathbf{P}^n$ (or equivalently, specific homogeneous polynomials $f_1, \ldots, f_m$), it is often easier to compute firstly the number

$$N_0 := \#\{[x_1 : \cdots : x_{n+1}] \in V(\mathbf{F}_q) \mid \exists i \in \{1, \ldots, n+1\}, x_i = 0\}$$

directly, and to compute secondly, for each choice $1 \leq i_1 < \cdots < i_r \leq m$, the number

$$N^{\times}_{i_1,\ldots,i_r} := \#\{[x_1 : \cdots : x_{n+1}] \in \mathbf{P}^n(\mathbf{F}_q) \mid$$

$$\forall i \in \{1,\ldots,n+1\},\ x_i \neq 0 \text{ and } \exists j \in \{i_1,\ldots,i_r\},\ f_j(x) = 0\},$$

which is $1/(q-1)$ times the number of rational points of the hypersurface of $(\mathbf{G}_m)^{n+1}$ defined by the product $f_{i_1} f_{i_2} \ldots f_{i_r}$.   Under this notation, our formula becomes

$$\#V(\mathbf{F}_q) = N_0 + \sum_{r=1}^{m} \sum_{1 \leq i_1 < \cdots < i_r \leq m} (-1)^{r+1} N^{\times}_{i_1,\ldots,i_r}.$$

Our calculations in Sections 3 and 4 also go in this manner.

We conclude this section by giving a formula for the number of $\mathbf{F}_q$-rational points of an arbitrary hypersurface of $(\mathbf{G}_m)^n$ in terms of Gauss sums.

Let us introduce a convention which we need to state the result. Let $M = (m_{ij})_{i,j}$ be an $n \times N$ matrix with coefficients in $\mathbf{Z}$. Then, M naturally defines the group homomorphism $\varphi(M) \colon (\widehat{\mathbf{F}_q^{\times}})^N \to (\widehat{\mathbf{F}_q^{\times}})^n$, explicitly expressed as

$$\varphi(M)((\chi_i)_{i=1,\ldots,N}) = (\chi_1^{m_{j1}} \ldots \chi_N^{m_{jN}})_{j=1,\ldots,n}.$$

We always regard elements of $(\widehat{\mathbf{F}_q^{\times}})^N$ and $(\widehat{\mathbf{F}_q^{\times}})^n$ as column vectors.

The following proposition gives a formula we are asking for.

PROPOSITION 3 ([2], [4]).   *Let n and N be positive integers, let $c_1,\ldots,c_N$ be elements of $\mathbf{F}_q^{\times}$, and let $R = (r_{ij})_{i,j} \in M_{n,N}(\mathbf{Z})$ be an $n \times N$ matrix. Define a polynomial $f(X_1,\ldots,X_n) \in \mathbf{F}_q[X_1,\ldots,X_n]$ by*

$$f(X_1,\ldots,X_n) = \sum_{j=1}^{N} c_j X_1^{r_{1j}} \ldots X_n^{r_{nj}}.$$

Then, the number of n-tuples $(x_1,\ldots,x_n) \in (\mathbf{F}_q^{\times})^n$ satisfying $f(x_1,\ldots,x_n) = 0$ equals

$$\frac{(q-1)^n}{q} + \frac{(q-1)^{n+1-N}}{q} \sum_{{}^t(\chi_1,\ldots,\chi_N) \in \mathrm{Ker}(\varphi(\tilde{R}))} \prod_{j=1}^{N} G(\chi_j^{-1})\chi_j(c_j),$$

where

$$\tilde{R} = \left(\frac{R}{1 \quad \ldots \quad 1} \right).$$

PROOF.   Lemma 1 (i) shows that

$$\sum_{x_1,\ldots,x_n \in \mathbf{F}_q^\times} \sum_{w \in \mathbf{F}_q} \theta(wf(x_1,\ldots,x_n))$$

$$= q\#\{(x_1,\ldots,x_n) \in (\mathbf{F}_q^\times)^n \mid f(x_1,\ldots,x_n) = 0\},$$

thus it suffices to calculate the left-hand side and divide the result by q. Because $\theta(0) = 1$ and because θ transforms addition to multiplication, the left-hand side equals

$$(q-1)^n + \sum_{x_1,\ldots,x_n,\,w \in \mathbf{F}_q^\times} \theta(wf(x_1,\ldots,x_n))$$

$$= (q-1)^n + \sum_{x_1,\ldots,x_n,\,w \in \mathbf{F}_q^\times} \prod_{j=1}^{N} \theta(c_j w x_1^{r_{1j}} \ldots x_n^{r_{nj}}).$$

Now, Proposition 2 shows that the second term equals

$$\frac{1}{(q-1)^N} \sum_{x_1,\ldots,x_n,\,w \in \mathbf{F}_q^\times} \prod_{j=1}^{N} \sum_{\chi_j \in \widehat{\mathbf{F}_q^\times}} G(\chi_j^{-1})\chi_j(c_j w x_1^{r_{1j}} \ldots x_n^{r_{nj}})$$

and by using the multiplicativity of characters, we know that it equals

$$\frac{1}{(q-1)^N} \sum_{\chi_1,\ldots,\chi_N \in \widehat{\mathbf{F}_q^\times}} \left\{ \prod_{j=1}^{N} G(\chi_j^{-1})\chi_j(c_j) \right.$$

$$\left. \prod_{i=1}^{n} \sum_{x_i \in \mathbf{F}_q^\times} (\chi_1^{r_{i1}} \ldots \chi_N^{r_{iN}})(x_i) \sum_{w \in \mathbf{F}_q^\times} (\chi_1 \ldots \chi_N)(w) \right\}.$$

Because of Lemma 1 (ii), each summand with respect to the outer sum vanishes unless $\chi_1^{r_{i1}} \ldots \chi_N^{r_{iN}} = \varepsilon$ for each $i = 1,\ldots,n$ and $\chi_1 \ldots \chi_N = \varepsilon$, that is, unless ${}^{\mathrm{t}}(\chi_1,\ldots,\chi_N) \in \mathrm{Ker}\,\varphi(\tilde{R})$; if it is the case, the summand equals $(q-1)^{n+1} \prod_{j=1}^{N} G(\chi_j^{-1})\chi_j(c_j)$. This completes the proof.

3.   The image of triple embedding $\mathbf{P}^1 \hookrightarrow \mathbf{P}^3$

In this section, we compute the number of rational points of $\mathbf{P}^1$ by identifying it as the image V of triple embedding $\mathbf{P}^1 \hookrightarrow \mathbf{P}^3$ and by following the strategy in the previous section.   Later, we compare the result with the obvious answer $\#\mathbf{P}^1(\mathbf{F}_q) = q + 1$.

The variety V is defined in $\mathbf{P}^3 = \text{Proj}(\mathbf{F}_q[x_1, x_2, x_3, x_4])$ by the following three polynomials:

$$f_1(x) = x_1 x_3 - x_2^2, \qquad f_2(x) = x_2 x_4 - x_3^2, \qquad f_3(x) = x_1 x_4 - x_2 x_3.$$

We follow the notation in Remark 2; in particular, we have

$$\#V(\mathbf{F}_q) = N_0 + N_1^\times + N_2^\times + N_3^\times - N_{12}^\times - N_{13}^\times - N_{23}^\times + N_{123}^\times. \qquad (1)$$

Firstly, we directly compute the number N_0. In our case, we easily see that

$$\{[x_1 : x_2 : x_3 : x_4] \in V(\mathbf{F}_q) \mid \exists i \in \{1, 2, 3, 4\}, \, x_i = 0\}$$
$$= \{[1 : 0 : 0 : 0], [0 : 0 : 0 : 1]\};$$

thus $N_0 = 2$.

Secondly, we compute the number

$$N_i^\times = \#\{[x_1 : x_2 : x_3 : x_4] \in \mathbf{P}^4(\mathbf{F}_q) \mid f_i(x) = 0 \text{ and } \forall j, \, x_j \neq 0\}$$

for $i \in \{1, 2, 3\}$. Although we could employ Proposition 3, a direct calculation is easy in this case. Namely, if $i = 1$, we may assume $x_4 = 1$, and after a free choice of $x_2, x_3 \in \mathbf{F}_q^\times$, the remaining $x_1 \in \mathbf{F}_q^\times$ is uniquely determined; thus we get $N_1^\times = (q-1)^2$. By a similar argument, we see that

$$N_1^\times = N_2^\times = N_3^\times = (q-1)^2.$$

Thirdly, we compute the number

$$N_{ij}^\times = \#\{[x_1 : x_2 : x_3 : x_4] \in \mathbf{P}^4(\mathbf{F}_q) \mid f_i(x) f_j(x) = 0 \text{ and } \forall j, \, x_j \neq 0\}$$

for $(i, j) \in \{(1, 2), (1, 3), (2, 3)\}$. Since

$$f_1(x) f_2(x) = x_1 x_2 x_3 x_4 - x_1 x_3^3 - x_2^3 x_4 + x_2^2 x_3^2,$$

Proposition 3 shows that

$$(q-1)N_{12}^\times = \frac{(q-1)^4}{q} + \frac{q-1}{q} \sum_{{}^t(\chi_1, \ldots, \chi_4) \in \text{Ker} \, \varphi(\widetilde{R_{12}})} \prod_{j=1}^{4} G(\chi_j^{-1}) \cdot \chi_2 \chi_3(-1), \qquad (2)$$

where

$$\widetilde{R_{12}} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 3 & 2 \\ 1 & 3 & 0 & 2 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Since an elementary linear algebra with coefficient in $\mathbf{Z}/(q-1)\mathbf{Z}$ shows that $\mathrm{Ker}\,\varphi(\widetilde{R_{12}}) = \{{}^{t}(\chi, \chi^{-1}, \chi^{-1}, \chi)\,|\,\chi \in \widehat{\mathbf{F}_q^\times}\}$, we have

$$(q-1)N_{12}^\times = \frac{(q-1)^4}{q} + \frac{q-1}{q}\sum_{\chi \in \widehat{\mathbf{F}_q^\times}} G(\chi^{-1})G(\chi)G(\chi^{-1})G(\chi).$$

With the aid of Proposition 1, we get (after dividing both sides by $q-1$)

$$N_{12}^\times = \frac{(q-1)^3}{q} + \frac{1}{q}\left(\sum_{\chi \in \widehat{\mathbf{F}_q^\times}\setminus\{\varepsilon\}} (q\chi(-1))^2 + (-1)^4\right)$$

$$= \frac{(q-1)^3}{q} + \frac{1}{q}\{q^2(q-2)+1\} = 2q^2 - 5q + 3. \qquad (3)$$

Similarly, since

$$f_2(x)f_3(x) = x_1 x_2 x_4^2 - x_2^2 x_3 x_4 - x_1 x_3^2 x_4 + x_2 x_3^3,$$

$(q-1)N_{23}^\times$ equals (2) with $\widetilde{R_{12}}$ replaced by

$$\widetilde{R_{13}} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 2 & 0 & 1 \\ 0 & 1 & 2 & 3 \\ 2 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

In fact, we may directly show that $\mathrm{Ker}\,\varphi(\widetilde{R_{12}}) = \mathrm{Ker}\,\varphi(\widetilde{R_{13}})$, and therefore we have $N_{13}^\times = N_{23}^\times$. Moreover, the symmetry shows $N_{23}^\times = N_{13}^\times$, and we have

$$N_{12}^\times = N_{13}^\times = N_{23}^\times = 2q^2 - 5q + 3.$$

Finally, we compute the number $N_{123}^\times$. Since

$$f_1(x)f_2(x)f_3(x) = x_1^2 x_2 x_3 x_4^2 - x_1^2 x_3^3 x_4 + x_1 x_2 x_3^4 - x_1 x_2^3 x_4^2 + x_2^4 x_3 x_4 - x_2^3 x_3^3,$$

Proposition 3 shows that $(q-1)N_{123}^\times$ equals

$$\frac{(q-1)^4}{q} + \frac{1}{q(q-1)}\sum_{{}^{t}(\chi_1,\ldots,\chi_6)\,\in\,\mathrm{Ker}(\varphi(\widetilde{R_{123}}))}\prod_{j=1}^{6} G(\chi_j^{-1})(\chi_2\chi_4\chi_6)(-1) \qquad (4)$$

with

$$\widetilde{R_{123}} = \begin{pmatrix} 2 & 2 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 3 & 4 & 3 \\ 1 & 3 & 4 & 0 & 1 & 3 \\ 2 & 1 & 0 & 2 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Again, an elementary linear algebra shows that $\mathrm{Ker}\,\varphi(\widetilde{R_{123}})$ equals

$$\{{}^{\mathrm t}(\chi_4^{-2}\chi_5^{-2}\chi_6^{-1}, \chi_4^2\chi_5^3\chi_6^2, \chi_4^{-1}\chi_5^{-2}\chi_6^{-2}, \chi_4, \chi_5, \chi_6)\,|\,\chi_4, \chi_5, \chi_6 \in \widehat{\mathbf{F}_q^\times}\}. \tag{5}$$

This time, we cannot simplify the sum in the second term of (4) as we did in (3). Instead, we rewrite this sum by using a more simple character sum.

By the definition of Gauss sums, the sum in the second term in (4) equals

$$\sum_{{}^{\mathrm t}(\chi_1,\dots,\chi_6) \in \mathrm{Ker}\,\varphi(\widetilde{R_{123}})} \prod_{i=1}^{6}\left(\sum_{t_i \in \mathbf{F}_q^\times} \theta(t_i)\chi_i^{-1}(t_i)\right)(\chi_4\chi_5\chi_6)(-1).$$

Now, the description (5) of $\mathrm{Ker}\,\varphi(\widetilde{R_{123}})$ shows that this equals

$$\sum_{\chi_4,\chi_5,\chi_6 \in \widehat{\mathbf{F}_q^\times}} \sum_{t_1,\dots,t_6 \in \mathbf{F}_q^\times} \left(\prod_{i=1}^{6}\theta(t_i)\right)\Bigg((\chi_4^2\chi_5^2\chi_6)(t_1)(\chi_4^{-2}\chi_5^{-3}\chi_6^{-2})(t_2)(\chi_4\chi_5^2\chi_6^2)(t_3)$$

$$\chi_4^{-1}(t_4)\chi_5^{-1}(t_5)\chi_6^{-1}(t_6)(\chi_4\chi_5\chi_6)(-1)\Bigg)$$

$$= \sum_{t_1,\dots,t_6 \in \mathbf{F}_q^\times} \theta\left(\sum_{i=1}^{6} t_i\right)\Bigg(\sum_{\chi_4 \in \widehat{\mathbf{F}_q^\times}} \chi_4(-t_1^2 t_2^{-2} t_3 t_4^{-1})$$

$$\sum_{\chi_5 \in \widehat{\mathbf{F}_q^\times}} \chi_5(-t_1^2 t_2^{-3} t_3^2 t_5^{-1}) \sum_{\chi_6 \in \widehat{\mathbf{F}_q^\times}} \chi_6(-t_1 t_2^{-2} t_3^2 t_6^{-1})\Bigg).$$

Applying Lemma 1 (iii), this equals

$$(q-1)^3 \sum_{t_1,t_2,t_3 \in \mathbf{F}_q^\times} \theta(t_1 + t_2 + t_3 - t_1^2 t_2^{-2} t_3 - t_1^2 t_2^{-3} t_3^2 - t_1 t_2^{-2} t_3^2),$$

and therefore, we get the equation

$$N_{123}^\times = \frac{(q-1)^3}{q} + \frac{q-1}{q}\sum_{t_1,t_2,t_3 \in \mathbf{F}_q^\times} \theta(t_1 + t_2 + t_3 - t_1^2 t_2^{-2} t_3 - t_1^2 t_2^{-3} t_3^2 - t_1 t_2^{-2} t_3^2).$$

Now, we summarize the calculation and we get the result.

Theorem 1. *Let* L *be the sum*

$$L = \sum_{t_1, t_2, t_3 \in \mathbf{F}_q^{\times}} \theta(t_1 + t_2 + t_3 - t_1^2 t_2^{-2} t_3 - t_1^2 t_2^{-3} t_3^2 - t_1 t_2^{-2} t_3^2).$$

Then, $\#V(\mathbf{F}_q) = -2q^2 + 6q - 1 + ((q-1)L - 1)/q.$

Proof. Substituting the results above in the equation (1), we get

$$\#V(\mathbf{F}_q) = 2 + 3(q-1)^2 - 3(2q^2 - 5q + 3) + (q-1)^3/q + (q-1)L/q.$$

As a corollary, we obtain an explicit description of the exponential sum L.

Corollary 1. $L = 2q^2 - 3q - 1.$

Proof. Since $\#V(\mathbf{F}_q) = \#\mathbf{P}^1(\mathbf{F}_q) = q + 1$, Theorem 1 gives an equation on L. Solving it gives the corollary.

This corollary can be viewed as an explicit description of the trace function of a rank-one l-adic sheaf.

Corollary 2. *Define a morphism* $f: \mathbf{G}_m^3 \to \mathbf{A}^1$ *by*

$$f(t_1, t_2, t_3) = t_1 + t_2 + t_3 - t_1^2 t_2^{-2} t_3 - t_1^2 t_2^{-3} t_3^2 - t_1 t_2^{-2} t_3^2,$$

and denote the Artin–Schreier sheaf on $\mathbf{A}^1$ *associated to* θ *by* $\mathscr{L}_\theta$. *Then, the equation*

$$\sum_{i=0}^{\infty} (-1)^i \operatorname{Tr}(\operatorname{Frob}; H_c^i(\mathbf{G}_m^3 \times_{\mathbf{F}_q} \overline{\mathbf{F}_q}, f^* \mathscr{L}_\theta)) = 2q^2 - 3q - 1.$$

holds.

Proof. The left-hand side equals L by the Grothendieck trace formula [8, III B 1.3].

Remark 3. Corollary 1 can be also rewritten in terms of general hypergeometric functions [7, 8.1], [6], which Lei Fu [5] calls GKZ hypergeometric sum. In fact, let A be the 3×6-matrix

$$A = \begin{pmatrix} 1 & 0 & 0 & 2 & 2 & 1 \\ 0 & 1 & 0 & -2 & -3 & -2 \\ 0 & 0 & 1 & 1 & 2 & 2 \end{pmatrix},$$

and let $\operatorname{Hyp}_\theta(x_1, x_2, x_3, x_4, x_5, x_6; \chi_1, \chi_2, \chi_3)$ denote the GKZ hypergeometric sum associated to A with parameters χ_1, χ_2, χ_3. Then the exponential sum L

coincides with the value $\text{Hyp}_\theta(1, 1, 1, -1, -1, -1; \varepsilon, \varepsilon, \varepsilon)$. In other words, let $\text{Hyp}_\theta(\chi_1, \chi_2, \chi_3)$ denote the l-adic GKZ hypergeometric sheaf associated to the matrix A with parameters $\chi_1, \chi_2, \chi_3 \in \widehat{\mathbf{F}_q^\times}$; this is a mixed perverse sheaf on $\mathbf{A}^6$ of weights ≤ 9 [5, Theorem 0.3 (i)]. Then, setting $x = (1, 1, 1, -1, -1, -1) \in \mathbf{A}^6$ and taking arbitrary geometric point $\bar{x}$ lying above x, we have

$$\text{Tr}(\text{Frob}_{\bar{x}}; \text{Hyp}_\theta(\varepsilon, \varepsilon, \varepsilon)_{\bar{x}}) = (-1)^9 L = -2q^2 + 3q + 1.$$

4. The image of Segre embedding $\mathbf{P}^1 \times \mathbf{P}^2 \hookrightarrow \mathbf{P}^5$

In this section, we give another example of counting rational points, the image V of the Segre embedding $\mathbf{P}^1 \times \mathbf{P}^2 \hookrightarrow \mathbf{P}^5$, and show that the character sum L defined in Theorem 1 again appears in the calculation. The variety V is defined in $\mathbf{P}^5 = \text{Proj}(\mathbf{F}_q[x_1, x_2, \ldots, x_6])$ by the following three polynomials:

$$f_1(x) = x_1 x_5 - x_2 x_4, \qquad f_2(x) = x_1 x_6 - x_3 x_4, \qquad f_3(x) = x_2 x_6 - x_3 x_5.$$

We again work under the notations in Remark 2. This time, the symmetry shows that $N_1^\times = N_2^\times = N_3^\times$ and that $N_{12}^\times = N_{23}^\times = N_{13}^\times$; we therefore have

$$\#V(\mathbf{F}_q) = N_0 + 3N_1^\times - 3N_{12}^\times + N_{123}^\times. \tag{6}$$

Firstly, we compute N_0. Although we may again describe all points in V_0 (or may, at the beginning, proceed not along Remark 2 but along the original Observation 1), it here seems easier to identify V as $\mathbf{P}^1 \times \mathbf{P}^2$. For a subscheme W of $\mathbf{P}^n$, let W_0 denote the set of rational points of W at least one of whose components is zero; therefore $N_0 = \#V_0$ under this notation. The identification $V = \mathbf{P}^1 \times \mathbf{P}^2$ gives

$$V_0 = \{(\mathbf{P}^1)_0 \times \mathbf{P}^2(\mathbf{F}_q)\} \cup \{\mathbf{P}^1(\mathbf{F}_q) \times (\mathbf{P}^2)_0\},$$

and it is easy to see that $\#(\mathbf{P}^1)_0 = 2$ and $\#(\mathbf{P}^2)_0 = 3q$. Now, we see that $N_0 = 2(q^2 + q + 1) + (q + 1)3q - 2 \cdot 3q = 5q^2 - q + 2$.

Secondly, the number $(q - 1)N_1^\times = \#\{x \in (\mathbf{F}_q^\times)^6 \mid f_1(x) = 0\}$ can be calculated just as in the previous section, and the result is $N_1^\times = (q - 1)^4$.

Thirdly, we compute the number $(q - 1)N_{12}^\times = \#\{x \in (\mathbf{F}_q^\times)^6 \mid f_1 f_2(x) = 0\}$. Since

$$f_1(x) f_2(x) = x_1^2 x_5 x_6 - x_1 x_3 x_4 x_5 - x_1 x_2 x_4 x_6 + x_2 x_3 x_4^2,$$

Proposition 3 shows that

$$(q - 1)N_{12}^\times = \frac{(q - 1)^6}{q} + \frac{(q - 1)^3}{q} \sum_{{}^t(\chi_1, \ldots, \chi_4) \in \text{Ker}\,\varphi(\widetilde{R_{12}})} \prod_{j=1}^4 G(\chi_j^{-1}) \cdot \chi_2 \chi_3(-1),$$

where

$$\widetilde{R_{12}} = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 2 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Since $\mathrm{Ker}\, \varphi(\widetilde{R_{12}}) = \{{}^{\mathrm{t}}(\chi, \chi^{-1}, \chi^{-1}, \chi) \,|\, \chi \in \widehat{\mathbf{F}_q^\times}\}$, we may calculate $N_{12}^\times$ as in (3) and we get

$$N_{12}^\times = \frac{(q-1)^5}{q} + \frac{(q-1)^2}{q}\{q^2(q-2) + 1\} = (q-1)^2(2q^2 - 5q + 3).$$

Finally, we compute the number $(q-1)N_{123}^\times = \#\{x \in (\mathbf{F}_q^\times)^6 \,|\, f_1(x)f_2(x)f_3(x) = 0\}$. Since $f_1(x)f_2(x)f_3(x)$ equals

$$x_1^2 x_2 x_5 x_6^2 - x_1^2 x_3 x_5^2 x_6 + x_1 x_3^2 x_4 x_5^2 - x_1 x_2^2 x_4 x_6^2 + x_2^2 x_3 x_4^2 x_6 - x_2 x_3^2 x_4^2 x_5,$$

Proposition 3 shows that

$$(q-1)N_{123}^\times = \frac{(q-1)^6}{q} + \frac{q-1}{q} \sum_{{}^{\mathrm{t}}(\chi_1,\ldots,\chi_6) \in \mathrm{Ker}(\varphi(\widetilde{R_{123}}))} \prod_{j=1}^{6} G(\chi_j^{-1})(\chi_2\chi_4\chi_6)(-1)$$

with

$$\widetilde{R_{123}} = \begin{pmatrix} 2 & 2 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 2 & 2 & 1 \\ 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 2 & 2 \\ 1 & 2 & 2 & 0 & 0 & 1 \\ 2 & 1 & 0 & 2 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

We may again show that $\mathrm{Ker}\, \varphi(\widetilde{R_{123}})$ equals

$$\{{}^{\mathrm{t}}(\chi_4^{-2}\chi_5^{-2}\chi_6^{-1}, \chi_4^2\chi_5^3\chi_6^2, \chi_4^{-1}\chi_5^{-2}\chi_6^{-2}, \chi_4, \chi_5, \chi_6) \,|\, \chi_4, \chi_5, \chi_6 \in \widehat{\mathbf{F}_q^\times}\};$$

this space is the same as what we treated in the previous subsection. Therefore, we may proceed the calculation just as before and show that, under the definition of L in Theorem 1,

$$N_{123}^\times = \frac{(q-1)^5}{q} + \frac{(q-1)^3}{q} L.$$

Let us summarize the calculations above; substituting the results in (6), we see that

$$\#V(\mathbf{F}_q) = -2q^4 + 10q^3 - 12q^2 + 10q + 1 + \{(q-1)^3 L - 1\}/q.$$

This equation and Corollary 1 give

$$\#V(\mathbf{F}_q) = q^3 + 2q^2 + 2q + 1 = (q+1)(q^2 + q + 1),$$

which coincides with $\#(\mathbf{P}^1 \times \mathbf{P}^2)(\mathbf{F}_q)$.

Acknowledgements

References

[1] P. Deligne, "La conjecture de Weil. I," Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307.

[2] J. Delsarte, "Nombre de solutions des équations polynomiales sur un corps fini," in Séminaire Bourbaki, 1948–1951, Exp. No. 39, 321–329.

[3] B. Dwork, "On the rationality of the zeta function of an algebraic variety," Amer. J. Math. **82** (1960), 631–648.

[4] E. Furtado Gomida, "On the theorem of Artin–Weil," Bol. Soc. Mat. São Paulo **4** (1949, 1951), 1–18.

[5] L. Fu, "ℓ-adic GKZ hypergeometric sheaf and exponential sums," arXiv:1208.1373v2.

[6] I. M. Gelfand and M. I. Graev, "Hypergeometric functions over finite fields," Dokl. Akad. Nauk **381**(6) (2001). English Translation in Doklady Math. **64** (2001), 402–406.

[7] I. M. Gelfand, M. I. Graev and V. S. Retakh, "Hypergeometric functions over an arbitrary field," Uspekhi Mat. Nauk **59**(5(359)) (2004), 29–100. English Translation in Russian Math. Surveys **59** (2004), 831–905.

[8] A. Grothendieck, "Cohomologie *l*-adique et Fonctions L," Lecture Notes in Math. **589**, Springer-Verlag, 1977.

[9] N. Koblitz, "The number of points on certain families of hypersurfaces over finite fields," Compositio Math. **48**(1) (1983), 3–23.

[10] T. Ono, "Sūron Josetsu," Shokabo, 1987. English Translation: "An introduction to algebraic number theory," The University Series in Mathematics, Plenum Press, New York, 1990.

[11] D. Wan, "Algorithmic theory of zeta functions over finite fields," in Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ. **44**, Cambridge Univ. Press (2008), 551–578.

[12] A. Weil, ''Numbers of solutions of equations in finite fields,'' Bull. Amer. Math. Soc. **55** (1949), 497–508.

Kazuaki Miyatani
Department of Mathematics
Graduate School of Science
Hiroshima University 1-3-1 *Kagamiyama*
Higashi-Hiroshima 739-8526, *Japan*
E-mail: miyatani@hiroshima-u.ac.jp

Makoto Sano
Department of Mathematics
Graduate School of Science
Hiroshima University 1-3-1 *Kagamiyama*
Higashi-Hiroshima 739-8526, *Japan*
E-mail: m126552@hiroshima-u.ac.jp