An explicit factorisation of the zeta functions of Dwork hypersurfaces

by

Philippe Goutet (Paris)

1. Introduction. Let n be an integer ≥ 3 and \mathbb{F}_q a finite field of characteristic $p \nmid n$. We consider the family of hypersurfaces of $\mathbb{F}_{\mathbb{F}_q}^{n-1}$ defined by

$$X_{\psi} \colon x_1^n + \dots + x_n^n - n\psi x_1 \dots x_n = 0$$
 (Dwork family),

where $\psi \in \mathbb{F}_q$ is a non-zero parameter. We will assume that X_{ψ} is non-singular, i.e. $\psi^n \neq 1$. We denote by $|X_{\psi}(\mathbb{F}_{q^r})|$ the number of points of X_{ψ} over an extension \mathbb{F}_{q^r} of degree r of \mathbb{F}_q ; the zeta function of X_{ψ} is defined by

$$Z_{X_{\psi}/\mathbb{F}_q}(t) = \exp\left(\sum_{r=1}^{+\infty} |X_{\psi}(\mathbb{F}_{q^r})| \frac{t^r}{r}\right).$$

When $q \equiv 1 \mod n$ (see [10, Theorem 7.2, p. 174]) and when n is prime (see [6, Theorem 9.5, p. 179]), it is shown that the zeta function of X_{ψ} takes the form

$$Z_{X_{\psi}/\mathbb{F}_q}(t) = \frac{(Q(t,\psi)R(q^{\rho}t^{\rho},\psi))^{(-1)^{n-1}}}{(1-t)(1-qt)\dots(1-q^{n-2}t)},$$

where ρ is the order of q in $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

In this formula, $Q(t, \psi)$ is a polynomial with integer coefficients of degree n-1. As proved by D. Wan (see [10, §7, eq. (14), p. 173]), this factor comes from the zeta function of the quotient Y_{ψ} of $X_{\psi} \otimes \mathbb{F}_{q^{\rho}}$ by the group $\{(\zeta_1, \ldots, \zeta_n) \in \mathbb{F}_{q^{\rho}} \mid \zeta_i^n = 1, \zeta_1 \ldots \zeta_n = 1\}$ (Wan calls Y_{ψ} a "singular mirror" of X_{ψ}):

$$Z_{Y_{\psi}/\mathbb{F}_q}(t) = \frac{Q(t,\psi)^{(-1)^{n-1}}}{(1-t)(1-qt)\dots(1-q^{n-2}t)}.$$

A simple equation of Y_{ψ} is $(y_1 + \cdots + y_n)^n = (n\psi)^n y_1 \dots y_n$.

²⁰¹⁰ Mathematics Subject Classification: Primary 14G10; Secondary 11G25, 14G15. Key words and phrases: zeta function factorisation, Dwork hypersurfaces, hypergeometric hypersurfaces.

The factor $R(t, \psi)$ is a polynomial with integer coefficients of degree

$$\frac{(n-1)^n + (-1)^n(n-1)}{n} - (n-1)$$

whose roots have absolute values $q^{-(n-4)/2}$. We are interested in describing the factorisation of R. Two approaches are possible: either predict, from a theoretical point of view, the existence of a factorisation of R, or look for explicit varieties with factors in their zeta functions appearing in R. Concerning the first approach, we refer to [8]. The second approach is brought up by Wan in [10, §7, p. 175] who mentions that it has been solved for n = 3, n = 4 (Dwork) and n = 5 (Candelas, de la Ossa, and Rodríguez-Villegas); a recent article of Katz [7] also takes up this subject from a different angle (1).

The aim of this article is to handle the case where n is a prime number ≥ 5 by using only properties of Gauss sums. The fact that n is prime allows us to restrict to the case $q \equiv 1 \mod n$ in view of Haessig's result [6, Theorem 9.5, p. 179] that, when n is prime,

$$R(qt, \psi) = R_{X_{\psi}/\mathbb{F}_{q^{\rho}}}(q^{\rho}t^{\rho}, \psi)^{1/\rho},$$

where ρ is the order of q in $(\mathbb{Z}/n\mathbb{Z})^{\times}$. More precisely, if we define $N_R(q^r)$ by $R(t,\psi) = \exp(\sum_{r=1}^{+\infty} N_R(q^r) \frac{t^r}{r})$, we will show the following result (Theorem 5.10).

Theorem. Let n be a prime number ≥ 5 such that $q \equiv 1 \mod n$. We can write

(1.1)
$$N_R(q^r) = q^{(n-5)/2} N_1(q^r) + q^{(n-7)/2} N_3(q^r) + \dots + N_{n-4}(q^r),$$
 where each $N_d(q^r)$ is a sum of some $|H_{d,i}(q^r)| - (q-1)^{l-1} q^{d+1-l}$, the $H_{d,i}$ being varieties of $\mathbb{A}^{d+2}_{\mathbb{F}_q}$ of hypergeometric type of odd dimension equal to d

with $1 \le d \le n-4$ (their equations are explicitly given in §5.3).

This equality in terms of number of points translates into a factorisation of the polynomial R in terms of the zeta function of the preceding $H_{d,i}(q^r)$.

This article is organised as follows. In §2, we recall the formulas concerning Gauss and Jacobi sums we will need. In §3, we compute, in terms of Gauss sums, the number of points of some varieties of hypergeometric type by a method similar to Koblitz' [9]. In §4, we recall the formula for the number of points of X_{ψ} , and in §5, we compare this formula with those from §3. Finally, in §6, we detail the cases n = 5 (already treated by Candelas, de la Ossa, and Rodríguez-Villegas in [4]) and n = 7. The assumptions that n = 1

⁽¹⁾ His results are in terms of traces of the Frobenius of the toric hypersurfaces $x_1 \dots x_n = \lambda y_1 \dots y_m$ over a hypergeometric sheave.

is prime and that $q \equiv 1 \mod n$ will only be used starting from §5 and §4.2 respectively.

Let us mention that our method does not give a geometric link between X_{ψ} and the varieties of hypergeometric type we consider.

2. Gauss and Jacobi sum formulas. In all this section, \mathbb{F}_q will be a finite field with q elements.

Let Ω be an algebraically closed field of characteristic zero, G a finite abelian group and $\hat{G} = \text{Hom}(G, \Omega^*)$ its character group. Let us recall the orthogonality formula

(2.1)
$$\frac{1}{|G|} \sum_{\varphi \in \hat{G}} \varphi(g) = \begin{cases} 1 & \text{if } g = e, \\ 0 & \text{if } g \neq e, \end{cases}$$

where e is the neutral element of G. We will use this formula when $G = \mathbb{F}_q$ or $G = \mathbb{F}_q^*$.

Let us now fix a non-trivial additive character $\varphi \colon \mathbb{F}_q \to \Omega^*$.

Proposition 2.1 (Orthogonality formula).

(2.2)
$$\frac{1}{q} \sum_{a \in \mathbb{F}_q} \varphi(ax) = \begin{cases} 1 & \text{if } x = 0, \\ 0 & \text{if } x \neq 0. \end{cases}$$

Proof. This results from (2.1) above and the fact that every additive character is of the form $x \mapsto \varphi(ax)$ for some $a \in \mathbb{F}_q$.

DEFINITION 2.2. If $\chi \colon \mathbb{F}_q^* \to \mathbf{\Omega}^*$ is a multiplicative character, we define the $Gauss\ sum$

$$G(\varphi, \chi) = \sum_{x \in \mathbb{F}_q^*} \varphi(x) \chi(x).$$

If **1** is the trivial character of \mathbb{F}_q^* , we have $G(\varphi, \mathbf{1}) = -1$.

PROPOSITION 2.3 (Reflection formula). If χ is a non-trivial character of \mathbb{F}_q^* ,

(2.3)
$$G(\varphi, \chi)G(\varphi, \chi^{-1}) = \chi(-1)q.$$

Proof. Let us recall the proof of this simple property (see also [2, Theorem 1.1.4(a), p. 10]). We have

$$G(\varphi,\chi)G(\varphi,\chi^{-1}) = \sum_{x,y \in \mathbb{F}_q^*} \varphi(x+y)\chi(x/y).$$

Making the change of variable x = yz, we obtain

$$G(\varphi, \chi)G(\varphi, \chi^{-1}) = \sum_{y, z \in \mathbb{F}_q^*} \varphi(y(1+z))\chi(z)$$
$$= \chi(-1)(q-1) + \sum_{z \in \mathbb{F}_q^*, z \neq -1} \left(\sum_{y \in \mathbb{F}_q^*} \varphi(y(1+z))\right)\chi(z).$$

We conclude by making the change of variable y' = y(1+z) and by using the orthogonality formula.

PROPOSITION 2.4 (Multiplication formula). Let $d \geq 1$ be an integer dividing q-1. If η is a character of \mathbb{F}_q^* ,

(2.4)
$$\frac{G(\varphi, \eta^d)}{\prod_{\chi^d = 1} G(\varphi, \eta\chi)} = \frac{\eta(d)^d}{\prod_{\chi^d = 1, \chi \neq 1} G(\varphi, \chi)}.$$

Proof. This seemingly simple formula does not seem to admit an elementary proof; we refer the reader to [2, Theorem 11.3.5, p. 355] for additional details. \blacksquare

DEFINITION 2.5. If (χ_1, \ldots, χ_r) is a finite sequence of characters of \mathbb{F}_q^* , we define the $Jacobi\ sum$

$$J(\chi_1, \dots, \chi_r) = \sum_{\substack{x_1, \dots, x_r \in \mathbb{F}_q^* \\ x_1 + \dots + x_r = 1}} \chi_1(x_1) \dots \chi_r(x_r).$$

PROPOSITION 2.6 (Link with Gauss sums). If χ_1, \ldots, χ_r are characters of \mathbb{F}_q^* not all trivial,

(2.5)
$$J(\chi_1, \dots, \chi_r) = \begin{cases} \frac{1}{q} \frac{G(\varphi, \chi_1) \dots G(\varphi, \chi_r)}{G(\varphi, \chi_1 \dots \chi_r)} & \text{if } \chi_1 \dots \chi_r = \mathbf{1}, \\ \frac{G(\varphi, \chi_1) \dots G(\varphi, \chi_r)}{G(\varphi, \chi_1 \dots \chi_r)} & \text{if } \chi_1 \dots \chi_r \neq \mathbf{1}. \end{cases}$$

Proof. Let us briefly recall the proof (see also [2, Theorem 10.3.1, p. 302]). The additive convolution of the functions χ_1, \ldots, χ_r is defined by

$$(\chi_1 * \cdots * \chi_r)(a) = \sum_{\substack{x_1 + \cdots + x_r = a \\ x_i \in \mathbb{F}_r^*}} \chi_1(x_1) \dots \chi_r(x_r).$$

It is equal to $(\chi_1 \dots \chi_r)(a)J(\chi_1, \dots, \chi_r)$ when $a \neq 0$. To compute the value when a = 0, we notice that the sum of $(\chi_1 * \dots * \chi_r)(a)$ over $a \in \mathbb{F}_q$ is 0 since at least one of the χ_i is non-trivial. Thus, $(\chi_1 * \dots * \chi_r)(0)$ is 0 if $\chi_1 \dots \chi_r \neq 1$ and is $-(q-1)J(\chi_1, \dots, \chi_r)$ if $\chi_1 \dots \chi_r = 1$. Moreover,

$$\prod_{i=1}^{r} G(\varphi, \chi_i) = \sum_{a \in \mathbb{F}_q} \varphi(a)(\chi_1 * \cdots * \chi_r)(a),$$

and so

$$\prod_{i=1}^{r} G(\varphi, \chi_i) = J(\chi_1, \dots, \chi_r) \cdot \begin{cases} G(\varphi, \chi_1 \dots \chi_n) & \text{if } \chi_1 \dots \chi_r \neq \mathbf{1}, \\ G(\varphi, \mathbf{1}) - (q - 1) & \text{if } \chi_1 \dots \chi_r = \mathbf{1}, \end{cases}$$

which shows the result.

PROPOSITION 2.7 (Fourier inversion formula). For every map $f: \mathbb{F}_q^* \to \Omega$,

(2.6)
$$\forall x \in \mathbb{F}_q^*, \quad f(x) = \frac{1}{q-1} \sum_{\eta \in \widehat{\mathbb{F}}_q^*} \left(\sum_{y \in \mathbb{F}_q^*} f(y) \eta^{-1}(y) \right) \eta(x).$$

Proof. This is a direct consequence of the orthogonality formulas for the characters of the abelian group \mathbb{F}_q^* .

Corollary 2.8. If $x \in \mathbb{F}_q^*$,

(2.7)
$$\varphi(x) = \frac{1}{q-1} \sum_{\eta \in \widehat{\mathbb{F}}_q^*} G(\varphi, \eta^{-1}) \eta(x).$$

- 3. Number of points of some varieties of hypergeometric type. In all of this section, n will be an integer ≥ 2 and \mathbb{F}_q a finite field with q elements.
- **3.1. Computation of the number of points.** We consider here some affine varieties of hypergeometric type for which we compute the number of points by using Gauss sums and taking inspiration from Koblitz [9, §5].

THEOREM 3.1. Let $k \geq l \geq 2$ be two integers and $\lambda \in \mathbb{F}_q^*$ a parameter. Denote by $H_{\lambda} \subset \mathbb{A}^{k+1}$ the affine variety defined by

$$\begin{cases} y^n = x_1^{\alpha_1} \dots x_k^{\alpha_k} (1 - x_1)^{\beta_1} \dots (1 - x_{l-1})^{\beta_{l-1}} (1 - x_l - \dots - x_k)^{\beta_l}, \\ \lambda x_1 \dots x_l = 1, \end{cases}$$

where α_i and β_i are integers ≥ 1 . The number of points of H_{λ} over \mathbb{F}_q is

$$|H_{\lambda}(\mathbb{F}_q)| = (q-1)^{l-1}q^{k-l} + \sum_{\substack{\chi^n = 1 \ \chi \neq 1}} \frac{1}{q-1} \sum_{\eta} N_{\lambda,\chi,\eta} \, \eta(\lambda),$$

where

$$N_{\lambda,\chi,\eta} = \frac{1}{q^{\nu}} \frac{G(\varphi,\chi^{\alpha_1}\eta) \dots G(\varphi,\chi^{\alpha_l}\eta) \, G(\varphi,\chi^{\beta_1}) \dots G(\varphi,\chi^{\beta_l}) G(\varphi,\chi^{\alpha_{l+1}}) \dots G(\varphi,\chi^{\alpha_k})}{G(\varphi,\chi^{\alpha_1+\beta_1}\eta) \dots G(\varphi,\chi^{\alpha_{l-1}+\beta_{l-1}}\eta) G(\varphi,\chi^{\alpha_l+\dots+\alpha_k+\beta_l}\eta)},$$

with ν denoting the number of trivial characters among those appearing in the denominator (namely, $\chi^{\alpha_j+\beta_j}\eta$ for $1 \leq j \leq l-1$ and $\chi^{\alpha_l+\cdots+\alpha_k+\beta_l}\eta$).

Proof. To simplify, we shall write $y^n = Q(x_1, \ldots, x_k)$ for the first equation defining H_{λ} . We have

$$|H_{\lambda}(\mathbb{F}_q)| = \sum_{\substack{x \in \mathbb{F}_q^k, \, y \in \mathbb{F}_q \\ y^n = Q(x) \\ \lambda x_1 \dots x_l = 1}} 1 = \sum_{\substack{x \in \mathbb{F}_q^k \\ \lambda x_1 \dots x_l = 1}} \sum_{\substack{y \in \mathbb{F}_q \\ y^n = Q(x)}} 1$$

with

$$|\{y \in \mathbb{F}_q \mid y^n = z\}| = \begin{cases} 1 & \text{if } z = 0, \\ 1 + \sum_{\substack{\chi^n = 1 \\ \chi \neq 1}} \chi(z) & \text{if } z \neq 0, \end{cases}$$

and thus

$$|H_{\lambda}(\mathbb{F}_{q})| = \sum_{\substack{x \in \mathbb{F}_{q}^{k} \\ \lambda x_{1} \dots x_{l} = 1 \\ Q(x) = 0}} 1 + \sum_{\substack{x \in \mathbb{F}_{q}^{k} \\ \lambda x_{1} \dots x_{l} = 1 \\ Q(x) \neq 0}} \left(1 + \sum_{\substack{\chi^{n} = 1 \\ \chi \neq 1}} \chi(Q(x))\right)$$

$$= \sum_{\substack{x \in \mathbb{F}_{q}^{k} \\ \lambda x_{1} \dots x_{l} = 1}} 1 + \sum_{\substack{x \in \mathbb{F}_{q}^{k} \\ \lambda x_{1} \dots x_{l} = 1 \\ Q(x) \neq 0}} \sum_{\substack{\chi^{n} = 1 \\ \chi \neq 1}} \chi(Q(x))$$

$$= (q - 1)^{l-1} q^{k-l} + \sum_{\substack{\chi^{n} = 1 \\ \chi \neq 1}} \sum_{\substack{x \in \mathbb{F}_{q}^{k} \\ \lambda x_{1} \dots x_{l} = 1 \\ Q(x) \neq 0}} \chi(Q(x))$$

$$= (q - 1)^{l-1} q^{k-l} + \sum_{\substack{\chi^{n} = 1 \\ \chi \neq 1}} \sum_{\substack{x \in \mathbb{F}_{q}^{k} \\ Q(x) \neq 0}} \chi(Q(x)) \delta_{\lambda x_{1} \dots x_{l}, 1},$$

where $\delta_{z,z'}$ is the Kronecker delta (= 1 if z = z' and = 0 otherwise). Because

$$\forall z, z' \in \mathbb{F}_q^*, \quad \delta_{z,z'} = \frac{1}{q-1} \sum_{\eta \in \widehat{\mathbb{F}}_z^*} \eta(z/z'),$$

we may write

$$|H_{\lambda}(\mathbb{F}_q)| = (q-1)^{l-1} q^{k-l}$$

$$+ \sum_{\substack{\chi^n = 1 \\ \chi \neq 1}} \frac{1}{q-1} \sum_{\eta \in \widehat{\mathbb{F}}_q^*} \Big(\sum_{\substack{x \in \mathbb{F}_q^k \\ Q(x) \neq 0}} \chi(Q(x)) \eta(x_1 \dots x_l) \Big) \eta(\lambda).$$

Let us compute $N_{\lambda,\chi,\eta} = \sum_{Q(x)\neq 0} \chi(Q(x)) \eta(x_1 \dots x_l)$. As α_i and β_i are > 0,

$$N_{\lambda,\chi,\eta} = \sum_{\substack{(x_1,\dots,x_k) \in (\mathbb{F}_q^*)^k \\ \forall i \leq l-1, x_i \neq 1 \\ x_l+\dots+x_k \neq 1}} (\chi^{\alpha_1}\eta)(x_1)\chi^{\beta_1}(1-x_1)\dots(\chi^{\alpha_{l-1}}\eta)(x_{l-1}) \\ \cdot \chi^{\beta_{l-1}}(1-x_{l-1})(\chi^{\alpha_l}\eta)(x_l)\chi^{\alpha_{l+1}}(x_{l+1})\dots\chi^{\alpha_k}(x_k) \\ \cdot \chi^{\beta_l}(1-x_l-\dots-x_k).$$

We recognize a product of Jacobi sums:

$$N_{\lambda,\chi,\eta} = J(\chi^{\alpha_1}\eta,\chi^{\beta_1})\dots J(\chi^{\alpha_{l-1}}\eta,\chi^{\beta_{l-1}})J(\chi^{\alpha_l}\eta,\chi^{\alpha_{l+1}},\dots,\chi^{\alpha_k},\chi^{\beta_l}).$$

By using formula (2.5), we deduce that

$$N_{\lambda,\chi,\eta} = \frac{1}{q^{\nu}} \frac{G(\varphi,\chi^{\alpha_1}\eta) \dots G(\varphi,\chi^{\alpha_l}\eta) G(\varphi,\chi^{\beta_1}) \dots G(\varphi,\chi^{\beta_l}) G(\varphi,\chi^{\alpha_{l+1}}) \dots G(\varphi,\chi^{\alpha_k})}{G(\varphi,\chi^{\alpha_1+\beta_1}\eta) \dots G(\varphi,\chi^{\alpha_{l-1}+\beta_{l-1}}\eta) G(\varphi,\chi^{\alpha_l+\dots+\alpha_k+\beta_l}\eta)},$$

with ν as defined in the theorem.

NOTATIONS. Let $N_{\lambda,\chi,\eta}$ be as in the previous theorem; we define

$$N_{\lambda,\chi} = \frac{1}{q-1} \sum_{\eta \in \widehat{\mathbb{F}}_q^*} N_{\lambda,\chi,\eta} \, \eta(\lambda) \quad \text{and} \quad N_{\lambda} = \sum_{\substack{\chi^n = 1 \\ \chi \neq 1}} N_{\lambda,\chi,\eta}.$$

COROLLARY 3.2. Assume that n is odd, none of the elements of the sequence $(\beta_1, \ldots, \beta_l, \alpha_{l+1}, \ldots, \alpha_k)$ is divisible by n, and for $1 \le b \le n-1$ the number of terms of the sequence $\equiv b \mod n$ is equal to the number of terms $\equiv -b \mod n$ (this implies that k is even). When these conditions are met, we say we have complete pairing. In this case,

$$N_{\lambda,\chi,\eta} = q^{k/2-\nu} \frac{G(\varphi,\chi^{\alpha_1}\eta) \dots G(\varphi,\chi^{\alpha_l}\eta)}{G(\varphi,\chi^{\alpha_1+\beta_1}\eta) \dots G(\varphi,\chi^{\alpha_{l-1}+\beta_{l-1}}\eta) G(\varphi,\chi^{\alpha_l+\dots+\alpha_k+\beta_l}\eta)},$$

where ν is the number of trivial characters appearing in the denominator.

Proof. This is an immediate consequence of the reflection formula (2.3):

$$G(\varphi, \chi^{\beta_1}) \dots G(\varphi, \chi^{\beta_l}) G(\varphi, \chi^{\alpha_{l+1}}) \dots G(\varphi, \chi^{\alpha_k}) = q^{k/2}.$$

(Note that because $\chi \neq \mathbf{1}$ and all α_i and β_j are $\not\equiv 0 \bmod n$, the characters appearing are all non-trivial, and so the reflection formula applies with $\chi(-1) = 1$ as n is odd.)

3.2. Link with some hypergeometric hypersurfaces. Assume that n is odd and that $\alpha_1 + \beta_1 \equiv 0 \mod n$. In that case, H_{λ} has the same number of points as the hypersurface of \mathbb{A}^k defined by

$$y^{n} = x_{2}^{\alpha_{2}} \dots x_{k}^{\alpha_{k}} (1 - x_{2})^{\beta_{2}} \dots (1 - x_{l-1})^{\beta_{l-1}} \cdot (1 - x_{l} - \dots - x_{k})^{\beta_{l+1}} (1 - \lambda x_{2} \dots x_{l})^{\beta_{1}}$$

without the points where $x_2 cdots x_l = 0$. In this way we recover a hypersurface of the same type as in [4, §11.1] when n = 5 (see also Example 6.1 below).

4. Number of points of the Dwork hypersurfaces. In all this section, n denotes an integer ≥ 3 and our aim is to compute the number of points of X_{ψ} and then organise it into an appropriate form to relate it to the number of points of varieties of hypergeometric type considered in §3.

To compute the number of points of X_{ψ} in terms of Gauss sums, one can use a method close to the one A. Weil used in [11] for the diagonal case $\psi = 0$; this is done for example in [9, Theorem 2, p. 13] and [10, §3]. After recalling this computation in §4.2, we will organise the terms in the same way as Candelas, de la Ossa and Rodríguez-Villegas did for the case n = 5 in [3, §9] and [4, §11], namely (see Theorem 4.10)

$$|X_{\psi}(\mathbb{F}_q)| = 1 + q + \dots + q^{n-2} + N_{\text{mirror}} + \sum N_s.$$

In Section 5, we will explain how each N_s is related to a $N_{\lambda} = |H_{\lambda}(\mathbb{F}_q)| - (q-1)^{l-1}q^{k-l}$ from Section 3 (here, $\lambda = 1/\psi^n$).

4.1. Preliminaries. The aim of this subsection is to set some useful notation. The groups $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^{\times}$ and \mathfrak{S}_n act on each $(s_1, \ldots, s_n) \in (\mathbb{Z}/n\mathbb{Z})^n$ satisfying $s_1 + \cdots + s_n = 0$ in the following way:

$$\forall j \in \mathbb{Z}/n\mathbb{Z}, \qquad j \cdot (s_1, \dots, s_n) = (s_1 + j, \dots, s_n + j);$$

$$\forall k \in (\mathbb{Z}/n\mathbb{Z})^{\times}, \qquad k \times (s_1, \dots, s_n) = (ks_1, \dots, ks_n);$$

$$\forall \sigma \in \mathfrak{S}_n, \qquad {}^{\sigma}(s_1, \dots, s_n) = (s_{\sigma^{-1}(1)}, \dots, s_{\sigma^{-1}(n)}).$$

DEFINITION 4.1. For $s = (s_1, \ldots, s_n) \in (\mathbb{Z}/n\mathbb{Z})^n$ with $s_1 + \cdots + s_n = 0$, we denote by

- $[s] = [s_1, \ldots, s_n]$ the class of (s_1, \ldots, s_n) mod the action of $\mathbb{Z}/n\mathbb{Z}$;
- $\langle s \rangle = \langle s_1, \dots, s_n \rangle$ the class of (s_1, \dots, s_n) mod the simultaneous actions of $\mathbb{Z}/n\mathbb{Z}$ and \mathfrak{S}_n ;
- \underline{s} the class of (s_1, \ldots, s_n) mod the simultaneous actions of $\mathbb{Z}/n\mathbb{Z}$, \mathfrak{S}_n and $(\mathbb{Z}/n\mathbb{Z})^{\times}$;
- γ_s the number of permutations of (s_1, \ldots, s_n) .

Remarks 4.2.

- The number γ_s only depends on \underline{s} , not on the choice of s.
- If all the s_i are equal, then $\gamma_s = 1$.
- If $\langle s \rangle = \langle 0, 1, \dots, n-1 \rangle$, then $\gamma_s = n!$ but the number of permutations of [s] is n!/n = (n-1)! (the 1/n comes from the fact that adding the same number to each coordinate amounts to a circular permutation).

The following lemma, which we will only use later (see Lemma 5.2), shows that, when n is prime, the number γ_s of permutations of (s_1, \ldots, s_n) is almost always the same as the number of permutations of $[s_1, \ldots, s_n]$.

LEMMA 4.3. Assume that n is prime. If $\langle s_1, \ldots, s_n \rangle \neq \langle 0, 1, \ldots, n-1 \rangle$, then γ_s is equal to the number of permutations of $[s_1, \ldots, s_n]$.

Proof. If there exists $j \in \mathbb{Z}/n\mathbb{Z}$ non-zero such that (s_1+j,\ldots,s_n+j) is a permutation of (s_1,\ldots,s_n) , then $\{s_1,\ldots,s_n\}$ is a non-empty subset of $\mathbb{Z}/n\mathbb{Z}$ stable under $x\mapsto x+j$ and thus equal to $\mathbb{Z}/n\mathbb{Z}$ as n is prime. Consequently, $\langle s\rangle = \langle 0,1,\ldots,n-1\rangle$.

REMARK 4.4. This proof shows that, when $\langle s \rangle \neq \langle 0, 1, \dots, n-1 \rangle$, the only $j \in \mathbb{Z}/n\mathbb{Z}$ such that there exists $\sigma \in \mathfrak{S}_n$ satisfying ${}^{\sigma}s = s + j$ is j = 0.

4.2. Formula for the number of points of X_{ψ} . The aim of this subsection is to prove Theorem 4.5 below, stated in a slightly different form by Koblitz in [9, §3]. From now on, we resume the notations and assumptions of the introduction: \mathbb{F}_q is a finite field, n an integer ≥ 3 such that $q \equiv 1 \mod n$, $\psi \in \mathbb{F}_q$ is a non-zero parameter (but we do not yet suppose that $\psi^n \neq 1$) and X_{ψ} is the hypersurface of $\mathbb{P}_{\mathbb{F}_q}^{n-1}$ given by $x_1^n + \cdots + x_n^n - n\psi x_1 \dots x_n = 0$.

Theorem 4.5 (Koblitz). We have

$$|X_{\psi}(\mathbb{F}_q)| = 1 + q + \dots + q^{n-2} + \frac{1}{q-1} \sum_{[s]} \sum_{\eta \in \widehat{\mathbb{F}}_q^*} \frac{1}{q^{\delta}} \Big(\prod_{i=1}^n G(\varphi, \chi^{-s_i} \eta^{-1}) \Big) G(\varphi, \eta^n) \eta \left(\frac{1}{(-n\psi)^n} \right),$$

where $\delta = 0$ if one of the $\chi^{s_i}\eta$ is trivial and $\delta = 1$ otherwise.

Proof. For completeness, and because it would be just as long to deduce our formula from Koblitz', we will recall the proof given in [9, §3].

Let
$$f(x) = x_1^n + \dots + x_n^n - n\psi x_1 \dots x_n$$
 and set

$$\nu_q(X_{\psi}) = |\{x \in \mathbb{F}_q^n \mid f(x) = 0\}|, \quad \nu_q^*(X_{\psi}) = |\{x \in (\mathbb{F}_q^*)^n \mid f(x) = 0\}|.$$

As $x_1
dots x_n$ is zero when one of the x_i is zero, we have $\nu_q(X_{\psi}) - \nu_q^*(X_{\psi}) = \nu_q(X_0) - \nu_q^*(X_0)$, i.e.

$$\nu_q(X_{\psi}) = \nu_q(X_0) + \nu_q^*(X_{\psi}) - \nu_q^*(X_0).$$

The computation of $\nu_q(X_0)$ is classical and goes back to A. Weil, so we will not recall it (see [11] or [2, Theorem 10.4.2, p. 304]). By using (2.5) to express everything in terms of Gauss sums and by the change of variable $\chi_i \mapsto \chi_i^{-1}$, we find that

(4.1)
$$\nu_{q}(X_{0}) = q^{n-1} + \frac{q-1}{q} \sum_{\substack{\chi_{i}^{n} = 1, \chi_{i} \neq 1 \\ \chi_{1} \dots \chi_{n} = 1}} \left(\prod_{i=1}^{n} G(\varphi, \chi_{i}^{-1}) \right).$$

We now need to compute $\nu_q^*(X_{\psi})$ and $\nu_q^*(X_0)$. Both computations rely on the same method, the only difference being that, when $\psi = 0$, the polynomial

f(x) is a sum of n monomials instead of n+1, which slightly changes the result. We will only give the details for $\nu_q^*(X_\psi)$ when $\psi \neq 0$.

The orthogonality formula (2.2) for additive characters shows that

$$\nu_q^*(X_\psi) = \frac{1}{q} \sum_{a \in \mathbb{F}_q} \sum_{x \in (\mathbb{F}_q^*)^n} \varphi(af(x))$$

$$= \frac{(q-1)^n}{q} + \frac{1}{q} \sum_{a \in \mathbb{F}_q^*} \sum_{x \in (\mathbb{F}_q^*)^n} \left(\prod_{i=1}^n \varphi(ax_i^n) \right) \varphi(-n\psi ax_1 \dots x_n).$$

We now express each $\varphi(...)$ in terms of Gauss sums thanks to (2.7):

$$\nu_{q}^{*}(X_{\psi}) = \frac{(q-1)^{n}}{q} + \frac{1}{q} \sum_{\eta_{1},\dots,\eta_{n+1} \in \widehat{\mathbb{F}}_{q}^{*}} \left(\prod_{i=1}^{n+1} G(\varphi, \eta_{i}^{-1}) \right) \left(\frac{1}{q-1} \sum_{a \in \mathbb{F}_{q}^{*}} (\eta_{1} \dots \eta_{n+1})(a) \right) \cdot \prod_{i=1}^{n} \left(\frac{1}{q-1} \sum_{x_{i} \in \mathbb{F}_{q}^{*}} (\eta_{i}^{n} \eta_{n+1})(x_{i}) \right) \eta_{n+1}(-n\psi).$$

By orthogonality formulas, the sums over a and the x_i are all non-zero (equal to q-1) if and only if

$$\begin{cases} \eta_1 \dots \eta_n \eta_{n+1} = \mathbf{1}, \\ \forall i \in [1; n], \quad \eta_i^n \eta_{n+1} = \mathbf{1}, \end{cases} \text{ i.e. } \exists \eta \in \widehat{\mathbb{F}}_q^*, \begin{cases} \eta_i = \chi_i \eta, \\ \chi_i^n = \mathbf{1} \text{ and } \chi_1 \dots \chi_n = \mathbf{1}, \\ \eta_{n+1} = \eta^{-n}. \end{cases}$$

The character η defined in this way is not unique; indeed, if η' and χ'_i are also solutions of the system, there exists χ satisfying $\chi^n = \mathbf{1}$ such that $\eta' = \chi^{-1}\eta$ and $\chi'_i = \chi\chi_i$ for all i. This means that if R is a representative set of the n-uples (χ_1, \ldots, χ_n) of characters mod the (χ, \ldots, χ) satisfying $\chi^n_i = \mathbf{1}$ and $\chi_1 \ldots \chi_n = \mathbf{1}$ with $\chi^n = \mathbf{1}$, then the map $(\chi_1, \ldots, \chi_n, \eta) \mapsto (\chi_1 \eta, \ldots, \chi_n \eta, \eta^{-n})$ is one-to-one from $R \times \widehat{\mathbb{F}}_q^*$ onto the set of (n+1)-uples $(\eta_1, \ldots, \eta_{n+1})$ satisfying the preceding conditions. It follows that if χ is a multiplicative character of order n,

$$(4.2) \quad \nu_q^*(X_\psi) = \frac{(q-1)^n}{q} + \frac{1}{q} \sum_{[s]} \sum_{\eta \in \widehat{\mathbb{F}}_q^*} \left(\prod_{i=1}^n G(\varphi, \chi^{-s_i} \eta^{-1}) \right) G(\varphi, \eta^n) \eta \left(\frac{1}{(-n\psi)^n} \right).$$

This ends the computation of $\nu_q^*(X_{\psi})$. By a similar method, we find

(4.3)
$$\nu_q^*(X_0) = \frac{(q-1)^n}{q} + \frac{q-1}{q} \sum_{\substack{\chi_i^n = 1 \\ \chi_1 \dots \chi_n = 1}} \prod_{i=1}^n G(\varphi, \chi_i^{-1}).$$

From (4.1) and (4.3), we obtain

$$\nu_{q}(X_{0}) - \nu_{q}^{*}(X_{0}) = q^{n-1} - \frac{(q-1)^{n}}{q} - \frac{q-1}{q} \sum_{\substack{\chi_{1}^{n} = 1 \\ \exists i, \chi_{i} = 1}} \prod_{i=1}^{n} G(\varphi, \chi_{i}^{-1})$$

$$= q^{n-1} - \frac{(q-1)^{n}}{q}$$

$$- \frac{q-1}{q} \sum_{\substack{(\chi_{1}, \dots, \chi_{n}) \bmod \{(\chi, \dots, \chi)\}\\ \chi_{i}^{n} = 1, \chi_{1} \dots \chi_{n} = 1}} \sum_{\substack{\eta \in \widehat{\mathbb{F}}_{q}^{*} \\ \eta^{n} = 1}} \prod_{i=1}^{n} G(\varphi, (\chi_{i}\eta)^{-1}).$$

Writing $\chi_i = \chi^{s_i}$ where χ is, as above, a character of order n, we transform the first sum into a sum over the [s] such that $s_i = 0$ for some i; finally, we combine the terms of this sum with those satisfying $\eta^n = \mathbf{1}$ in (4.2) above for $\nu_q^*(X_{\psi})$. As $G(\varphi, \mathbf{1}) = -1$, we have, with δ as defined in the theorem,

$$\begin{split} \nu_q(X_{\psi}) &= \nu_q^*(X_{\psi}) + \nu_q(X_0) - \nu_q^*(X_0) \\ &= q^{n-1} + \sum_{[s]} \sum_{\eta \in \widehat{\mathbb{F}}_q^*} \frac{1}{q^{\delta}} \Big(\prod_{i=1}^n G(\varphi, \chi^{-s_i} \eta^{-1}) \Big) G(\varphi, \eta^n) \eta \bigg(\frac{1}{(-n\psi)^n} \bigg). \end{split}$$

By counting the number of zeros in the projective space instead of the affine space, we obtain the announced formula.

4.3. Reorganisation of the terms. We keep the assumptions and notations of §4.2 and suppose that n is odd. The aim of this subsection is to write the formula obtained for $|X_{\psi}(\mathbb{F}_q)|$ in Theorem 4.5 in terms of some coefficients $\beta_{(s_1,\ldots,s_n),\chi,\eta}$ which we now define.

DEFINITION 4.6. Let $(s_1, \ldots, s_n) \in (\mathbb{Z}/n\mathbb{Z})^n$ with $s_1 + \cdots + s_n = 0$. If χ is a multiplicative character of \mathbb{F}_q^* of order n and if η is a character of \mathbb{F}_q^* , we set

$$(4.4) \qquad \beta_{(s_1,\dots,s_n),\chi,\eta} = q^{(n+1)/2-z-\delta} \frac{G(\varphi,\eta)G(\varphi,\chi\eta)\dots G(\varphi,\chi^{n-1}\eta)}{G(\varphi,\chi^{s_1}\eta)\dots G(\varphi,\chi^{s_n}\eta)},$$

where z denotes the number of trivial characters in the finite sequence $(\chi^{s_1}\eta, \ldots, \chi^{s_n}\eta)$ and where $\delta = 0$ if $z \neq 0$ and $\delta = 1$ if z = 0 (this is the same δ as in Theorem 4.5).

Proposition 4.7. With the above assumptions,

$$\frac{1}{q^{\delta}} \left(\prod_{i=1}^{n} G(\varphi, \chi^{-s_i} \eta^{-1}) \right) G(\varphi, \eta^n) \eta \left(\frac{1}{(-n\psi)^n} \right) = \beta_{(s_1, \dots, s_n), \chi, \eta} \eta \left(\frac{1}{\psi^n} \right).$$

Proof. Invoking the reflection formula (2.3), we obtain

$$\prod_{i=1}^n G(\varphi, \chi^{-s_i} \eta^{-1}) = q^{n-z} \frac{\eta(-1)^n}{G(\varphi, \chi^{s_1} \eta) \dots G(\varphi, \chi^{s_n} \eta)},$$

and, using the multiplication formula (2.4), we get, as n is odd,

$$G(\varphi, \eta^n) = \frac{\eta(n)^n}{q^{(n-1)/2}} G(\varphi, \eta) G(\varphi, \chi \eta) \dots G(\varphi, \chi^{n-1} \eta).$$

From these two formulas, we deduce the result at once.

The coefficients β defined above satisfy the following three compatibility relations with respect to the actions of the groups $\mathbb{Z}/n\mathbb{Z}$, \mathfrak{S}_n and $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

Lemma 4.8. With the above notations and assumptions,

$$(4.5) \forall \sigma \in \mathfrak{S}_n, \beta_{(s_{\sigma(1)},\dots,s_{\sigma(n)}),\chi,\eta} = \beta_{(s_1,\dots,s_n),\chi,\eta};$$

$$(4.6) \forall j \in \mathbb{Z}, \beta_{(s_1+j,\ldots,s_n+j),\chi,\eta} = \beta_{(s_1,\ldots,s_n),\chi,\chi^j\eta};$$

$$(4.7) \forall k \in (\mathbb{Z}/n\mathbb{Z})^{\times}, \beta_{(ks_1,\dots,ks_n),\chi,\eta} = \beta_{(s_1,\dots,s_n),\chi^k,\eta}.$$

Proof. Formula (4.5) results immediately from the definition of β . As for (4.6) and (4.7), we note that the product $G(\varphi, \eta)G(\varphi, \chi\eta)\dots G(\varphi, \chi^{n-1}\eta)$ in (4.4) stays the same if we change η into $\chi^j\eta$, or χ into χ^k with k prime to n.

PROPOSITION 4.9. Under the above assumptions, the following quantities only depend on $\langle s \rangle$ (as well as on the choice of χ) and of \underline{s} respectively and not on the choice of the representative (s_1, \ldots, s_n) :

$$N_{\langle s \rangle, \chi} = \frac{1}{q-1} \sum_{\eta \in \widehat{\mathbb{F}}_q^*} \beta_{(s_1, \dots, s_n), \chi, \eta} \eta \left(\frac{1}{\psi^n} \right), \quad N_{\underline{s}} = \gamma_s \sum_{\langle s' \rangle \in \underline{s}} N_{\langle s' \rangle, \chi}.$$

Proof. For $N_{[s],\chi}$, we just use (4.6) and the fact that $\eta \mapsto \chi^j \eta$ is a one-to-one map of $\widehat{\mathbb{F}}_q^*$ onto itself when $j \in \mathbb{Z}/n\mathbb{Z}$. For $N_{\underline{s}}$, we use (4.7) and the fact that $\chi \mapsto \chi^k$ is a one-to-one map of $\{\chi \in \widehat{\mathbb{F}}_q^* \mid \chi^n = \mathbf{1}\}$ onto itself if $k \in (\mathbb{Z}/n\mathbb{Z})^{\times}$.

We deduce the following result.

Theorem 4.10. Under the preceding assumptions, we have

$$|X_{\psi}(\mathbb{F}_q)| = 1 + q + \dots + q^{n-2} + \sum_{s} N_{\underline{s}}.$$

REMARK 4.11. As we will see in §4.4 below, $N_0 = N_{\text{mirror}}$ and, when X_{ψ} is non-singular (i.e. when $\psi^n \neq 1$), $N_{(0,1,2,\dots,n-1)} = 0$.

4.4. Identification of some of the factors. We keep the assumptions and notations of §4.3. Let us recall that Y_{ψ} denotes the "singular mirror" of X_{ψ} , as specified in the introduction, and we write $N_{\text{mirror}} = |Y_{\psi}(\mathbb{F}_q)| - (1 + q + \cdots + q^{n-2})$.

Theorem 4.12 (Wan). $N_{\underline{0}} = N_{\text{mirror}}$.

Proof. See [10, §4]; note that the result is not known when $q \not\equiv 1 \mod n$, unless n is prime (see [6]).

Recall that, in this section, the only assumption on ψ is that $\psi \neq 0$.

Lemma 4.13. We have

$$N_{(0,1,2,\dots,n-1),\chi} = \begin{cases} 0 & \text{if } \psi^n \neq 1, \\ q^{(n-1)/2} & \text{if } \psi^n = 1, \end{cases}$$

and so the term $N_{(0,1,2,\dots,n-1)} = (n-1)! N_{(0,1,2,\dots,n-1),\chi}$ does not contribute to the zeta function $Z_{X_{\psi}/\mathbb{F}_q}(t)$ when $\psi^n \neq 1$, and contributes $(1-q^{(n-1)/2}t)^{-(n-1)!}$ when $\psi^n = 1$.

Proof. When $\langle s_1, \ldots, s_n \rangle = \langle 0, 1, \ldots, n-1 \rangle$, we have

$$G(\varphi, \chi^{s_1}\eta) \dots G(\varphi, \chi^{s_n}\eta) = G(\varphi, \eta)G(\varphi, \chi\eta) \dots G(\varphi, \chi^{n-1}\eta).$$

Moreover, the number z of trivial characters in the sequence $(\eta, \chi \eta, \dots, \chi^{n-1} \eta)$ is equal to $1 - \delta$ with the notations of Definition 4.6, and thus

$$\beta_{(0,1,\dots,n-1),\chi,\eta} = q^{(n-1)/2}.$$

Consequently,

$$N_{\langle 0,1,2,\dots,n-2,n-1\rangle,\chi} = \frac{q^{(n-1)/2}}{q-1} \sum_{\eta \in \widehat{\mathbb{F}}_q^*} \eta\bigg(\frac{1}{\psi^n}\bigg),$$

and we conclude by using an orthogonality formula.

Remark 4.14. A similar result was given by Candelas, de la Ossa and Rodríguez-Villegas when q = p and n = 5 (see [3, §9.3]).

5. Link between the number of points. In all this section, we will assume that n is a prime ≥ 5 and $q \equiv 1 \mod n$. We will only add the assumption that $\psi^n = 1$ in Theorem 5.10.

The aim of this section is to show (in §5.4) formula (1.1) of the introduction. More precisely, we shall show, in Theorem 5.7, that each $N_{\underline{s}}$ (with $\underline{s} \neq \underline{0}$) (²) appearing in Theorem 4.10 is equal, up to a multiplicative integer

⁽²⁾ Note that there is no $\underline{s} \neq \underline{0}$ when n = 3; this explains the assumption that $n \geq 5$.

constant and a power of q, to a term of the form

(5.1)
$$N_{\lambda} = \sum_{\substack{\chi^{n} = 1 \\ \chi \neq 1}} N_{\lambda,\chi} = \sum_{\substack{\chi^{n} = 1 \\ \chi \neq 1}} \frac{1}{q - 1} \sum_{\eta \in \widehat{\mathbb{F}}_{q}^{*}} N_{\lambda,\chi,\eta} \, \eta(\lambda),$$

where $\lambda = 1/\psi^n$ and $N_{\lambda,\chi,\eta}$ is given by Corollary 3.2.

The crucial point is, starting from a given \underline{s} , to find the relevant integers α_i and β_j . For that, we define in §5.2 integers v_i and w_i from which we then define α_i and β_j in §5.3. But before this, we start with a divisibility result useful for the main result.

5.1. A divisibility result. The aim of this subsection is to show that the integer γ_s (from Definition 4.1) is divisible by

$$K_s = |\{k \in (\mathbb{Z}/n\mathbb{Z})^{\times} \mid [ks_1, \dots, ks_n] \text{ is a permutation of } [s_1, \dots, s_n]\}|.$$

This result is crucial in Theorem 5.7 to ensure that the quotient γ_s/K_s is an integer. Note that K_s only depends on \underline{s} , not on the choice of s.

DEFINITION 5.1. Given $s \in (\mathbb{Z}/n\mathbb{Z})^n$ such that $s_1 + \cdots + s_n = 0$, we consider the following subgroups of \mathfrak{S}_n :

$$S'_{s} = \{ \sigma \in \mathfrak{S}_{n} \mid {}^{\sigma}s = s \},$$

$$S_{s} = \{ \sigma \in \mathfrak{S}_{n} \mid [{}^{\sigma}s] = [s] \},$$

$$S_{\bar{s}} = \{ \sigma \in \mathfrak{S}_{n} \mid [{}^{\sigma}s] \in (\mathbb{Z}/n\mathbb{Z})^{\times} \cdot [s] \}.$$

With these notations, $[\mathfrak{S}_n : S'_s]$ is the number γ_s of permutations of (s_1, \ldots, s_n) , whereas $[\mathfrak{S}_n : S_s]$ is the number of permutations of $[s_1, \ldots, s_n]$.

LEMMA 5.2. When $\underline{s} \neq \underline{0}$, the integer K_s divides $[\mathfrak{S}_n : S_s]$. Hence, when additionally $\langle s \rangle \neq \langle 0, 1, \dots, n-1 \rangle$, K_s divides $\gamma_s = [\mathfrak{S}_n : S_s'] = [\mathfrak{S}_n : S_s]$.

Proof. We remark that

$$K_s = \frac{|S_{\bar{s}}|}{|S_s|} \cdot |\{k \in (\mathbb{Z}/n\mathbb{Z})^{\times} \mid [ks] = [s]\}|.$$

As $[s] \neq [0, \ldots, 0]$, we have $|\{k \in (\mathbb{Z}/n\mathbb{Z})^{\times} \mid [ks] = [s]\}| = 1$ and so $[\mathfrak{S}_n : S_s] = [\mathfrak{S}_n : S_{\bar{s}}] \cdot K_s$. When furthermore $\langle s \rangle \neq \langle 0, 1, \ldots, n-1 \rangle$, we have $\gamma_s = [\mathfrak{S}_n : S_s]$ by Lemma 4.3, hence the result. \blacksquare

5.2. Transformation of the β **coefficients.** In order to relate $N_{\underline{s}}$ to a certain N_{1/ψ^n} in §5.3, we must first change the formula giving $\beta_{(s_1,\ldots,s_n),\chi,\eta}$.

NOTATIONS. Let $(s_1, \ldots, s_n) \in (\mathbb{Z}/n\mathbb{Z})^n$ with $s_1 + \cdots + s_n = 0$. For each $b \in \mathbb{Z}/n\mathbb{Z}$, define $k(b) = |\{i \mid s_i = b\}|$. We have

$$\sum_{b\in\mathbb{Z}/n\mathbb{Z}}k(b)b=0\quad\text{and}\quad\sum_{b\in\mathbb{Z}/n\mathbb{Z}}k(b)=n.$$

We also set $n' = |\{b \in \mathbb{Z}/n\mathbb{Z} \mid k(b) \neq 0\}|$ and m = n - n'.

Remarks 5.3.

- (a) The integer n' satisfies $1 \le n' \le n$ and we have n' = 1 if and only if $[s] = [0, \dots, 0]$, while n' = n if and only if $\langle s \rangle = \langle 0, 1, \dots, n-1 \rangle$.
- (b) As *n* is prime, $n' \neq 2$. Indeed, if $k_1b_1 + k_2b_2 = 0$ with $k_1, k_2 \geq 1$ and $k_1 + k_2 = n$, then $k_1 \not\equiv 0 \mod n$ and $k_1(b_1 b_2) = 0$, hence $b_1 = b_2$.
- (c) As n is odd, $n' \neq n-1$. Indeed, let s_1, \ldots, s_{n-1} be distinct elements of $\mathbb{Z}/n\mathbb{Z}$ and denote by s_n the element of $\mathbb{Z}/n\mathbb{Z}$ not appearing in this sequence; as n is odd, we have $s_1 + \cdots + s_n = 0$, and so $2s_1 + \cdots + s_{n-1} = s_1 s_n \neq 0$.
- (d) Thus, if $\langle s \rangle \neq \langle 0, 1, \dots, n-1 \rangle$, then $m \geq 2$, and if moreover $[s] \neq [0]$, then $2 \leq m \leq n-3$.

Theorem 5.4. With the preceding notations,

$$\beta_{(s_1,\dots,s_n),\chi,\eta} = q^{(n-1)/2-\nu} \frac{\prod_{b \in \mathbb{Z}/n\mathbb{Z}, k(b)=0} G(\varphi,\chi^b \eta)}{\prod_{b \in \mathbb{Z}/n\mathbb{Z}, k(b)\neq 0} G(\varphi,\chi^b \eta)^{k(b)-1}},$$

where $\nu = 0$ unless there exists b such that $\chi^b \eta = 1$ and $k(b) \neq 0$, in which case $\nu = k(b) - 1$.

Proof. From the definition of $\beta_{(s_1,\ldots,s_n),\chi,\eta}$ (Definition 4.6), we have

$$\beta_{(s_1,\dots,s_n),\chi,\eta} = q^{(n+1)/2-z-\delta} \frac{\prod_{b \in \mathbb{Z}/n\mathbb{Z}} G(\varphi,\chi^b \eta)}{\prod_{b \in \mathbb{Z}/n\mathbb{Z}} G(\varphi,\chi^b \eta)^{k(b)}}$$
$$= q^{(n+1)/2-z-\delta} \frac{\prod_{k(b)=0} G(\varphi,\chi^b \eta)}{\prod_{k(b)\neq 0} G(\varphi,\chi^b \eta)^{k(b)-1}}.$$

We now have to show that $z+\delta=1+\nu$. Recall that z is the number of trivial characters in the finite sequence $(\chi^{s_1}\eta,\ldots,\chi^{s_n}\eta)$ and that $\delta=0$ if $z\neq 0$ and $\delta=1$ if z=0. When z=0, we have $\delta=1$ and $\nu=0$, hence $z+\delta=1+\nu$. When $z\neq 0$, there exists a unique $b\in \mathbb{Z}/n\mathbb{Z}$ such that $\eta=\chi^{-b}$; we thus have z=k(b), $\delta=0$ and $\nu=k(b)-1$, hence $z+\delta=1+\nu$.

REMARK 5.5. Let (v_1, \ldots, v_m) be an enumeration of the $b \in \mathbb{Z}/n\mathbb{Z}$ such that k(b) = 0 and let (w_1, \ldots, w_m) be an enumeration of the $b \in \mathbb{Z}/n\mathbb{Z}$ such that $k(b) \geq 2$, each repeated with multiplicity k(b) - 1. The formula of Theorem 5.4 can be rewritten as

$$(5.2) \beta_{(s_1,\ldots,s_n),\chi,\eta} = q^{(n-1)/2-\nu} \frac{G(\varphi,\chi^{v_1}\eta)\ldots G(\varphi,\chi^{v_m}\eta)}{G(\varphi,\chi^{w_1}\eta)\ldots G(\varphi,\chi^{w_m}\eta)},$$

where ν is the number of trivial characters appearing in the denominator.

LEMMA 5.6. With the notations of the preceding remark,

$$v_1 + \dots + v_m \equiv w_1 + \dots + w_m \mod n.$$

Proof. This identity can be rewritten as

$$\sum_{k(b)=0} b = \sum_{k(b) \ge 1} (k(b) - 1)b, \text{ i.e. } \sum_{b} b = \sum_{b} k(b)b.$$

We conclude by noting that $\sum_{b\in\mathbb{Z}/n\mathbb{Z}} k(b)b = 0$ and that, because n is odd, $\sum_{b\in\mathbb{Z}/n\mathbb{Z}} b = 0$.

5.3. Link with the hypergeometric varieties. We now establish the link between X_{ψ} and the varieties of hypergeometric type from §3.

THEOREM 5.7. Let \underline{s} be distinct from the class of (0, 1, ..., n-1) and of (0, ..., 0). If s is a representative of \underline{s} , assume that there exist sequences $(v_1, ..., v_m)$ and $(w_1, ..., w_m)$ of elements of $\mathbb{Z}/n\mathbb{Z}$ as in Remark 5.5 and an even integer $m' \leq m-2$ such that

$$\forall i \in [1; m'/2], \quad w_{2i-1} - v_{2i-1} \equiv -(w_{2i} - v_{2i}) \bmod n.$$

We consider the affine variety H_{1/ψ^n} of dimension 2m - m' - 3 given by

$$\begin{cases} y^n = x_1^{v_1} \dots x_m^{v_m} x_{m+1}^{v_{m'+1}-w_{m'+1}} \dots x_{2m-m'-2}^{v_{m-2}-w_{m-2}} (1-x_1)^{w_1-v_1} \\ \dots (1-x_{m-1})^{w_{m-1}-v_{m-1}} (1-x_m-\dots-x_{2m-m'-2})^{v_{m-1}-w_{m-1}}, \\ x_1 \dots x_m = \psi^n. \end{cases}$$

(In this formula, we replace the exponents by their representatives in [1; n].) It is a variety of the form considered in Corollary 3.2 and we have, using the notations of $\S 3$,

$$N_{\underline{s}} = \frac{\gamma_s}{K_s} \, q^{(n+1)/2 - (2m-m')/2} N_{1/\psi^n} \quad \text{ where } \gamma_s/K_s \in \mathbb{N} \text{ by Lemma 5.2.}$$

Proof. As \underline{s} is distinct from the class of $(0,1,\ldots,n-1)$, we have $m \geq 2$ (see Remark 5.3(d)). The variety we consider is the one introduced in Theorem 3.1 with $l=m, \ k=2m-m'-2$ and

$$\begin{split} &\alpha_1 = v_1, \ \dots, \ \alpha_m = v_m; \\ &\alpha_{m+1} = v_{m'+1} - w_{m'+1}, \ \dots, \ \alpha_{2m-m'-2} = v_{m-2} - w_{m-2}; \\ &\beta_1 = w_1 - v_1, \ \dots, \ \beta_{m-1} = w_{m-1} - v_{m-1}, \qquad \beta_m = v_{m-1} - w_{m-1}. \end{split}$$

According to the pairing assumption on the v_i and w_i and to Lemma 5.6, we have

$$v_{m'+1}+\cdots+v_m=w_{m'+1}+\cdots+w_m\quad\text{in }\mathbb{Z}/n\mathbb{Z},$$
 and thus $\alpha_m+\alpha_{m+1}+\cdots+\alpha_{2m-m'-2}+\beta_m\equiv w_m \bmod n.$ Moreover,
$$\alpha_1+\beta_1\equiv w_1 \bmod n,\ \ldots,\ \alpha_{m-1}+\beta_{m-1}\equiv w_{m-1} \bmod n;$$

$$\beta_1+\beta_2\equiv 0 \bmod n,\ \ldots,\ \beta_{m'-1}+\beta_{m'}\equiv 0 \bmod n;$$

$$\alpha_{m+1}+\beta_{m'+1}\equiv 0 \bmod n,\ \ldots,\ \alpha_{2m-m'-2}+\beta_{m-2}\equiv 0 \bmod n;$$

$$\beta_{m-1}+\beta_m\equiv 0 \bmod n.$$

The last three lines show that we have complete pairing (in the sense of Corollary 3.2) of the sequence $(\beta_1, \ldots, \beta_m, \alpha_{m+1}, \ldots, \alpha_{2m-m'-2})$; these elements are $\not\equiv 0 \mod n$ as $v_i \not\equiv w_i \mod n$, and so

$$N_{1/\psi^n,\chi,\eta} = q^{(2m-m'-2)/2-\nu} \frac{G(\varphi,\chi^{v_1}\eta)\dots G(\varphi,\chi^{v_m}\eta)}{G(\varphi,\chi^{w_1}\eta)\dots G(\varphi,\chi^{w_m}\eta)}.$$

Hence, by comparing with (5.2), we obtain

$$\beta_{(s_1,\dots,s_n),\chi,\eta} = q^{(n+1)/2 - (2m - m')/2} N_{1/\psi^n,\chi,\eta}.$$

Multiplying this equality by $\frac{1}{q-1}\eta(1/\psi^n)$ and summing over $\eta\in\widehat{\mathbb{F}}_q^*$, we get

$$N_{\langle s \rangle, \chi} = q^{(n+1)/2 - (2m - m')/2} N_{1/\psi^n, \chi}.$$

We now sum the preceding formula over $k \in [1; n-1]$ with χ replaced by χ^k . Noting that $N_{\langle s \rangle, \chi^k} = N_{\langle ks \rangle, \chi}$ (see (4.7)), we obtain

$$\sum_{k=1}^{n-1} N_{\langle ks \rangle,\chi} = q^{\frac{n+1}{2} - \frac{2m-m'}{2}} N_{1/\psi^n}.$$

The left hand side is equal to $K_s \sum_{\langle s' \rangle \in \underline{s}} N_{\langle s' \rangle, \chi} = (K_s/\gamma_s) N_{\underline{s}}$. As $[s] \neq [0]$, Lemma 5.2 shows that γ_s/K_s is an integer. The result is hence proved.

REMARK 5.8. When m' = m - 2, we have $v_{m-1} - w_{m-1} = w_m - v_m$ by Lemma 5.6 and the equation of the variety simplifies greatly:

$$H_{1/\psi^n}: \begin{cases} y^n = x_1^{v_1} \dots x_m^{v_m} (1-x_1)^{w_1-v_1} \dots (1-x_m)^{w_m-v_m}, \\ x_1 \dots x_m = \psi^n. \end{cases}$$

5.4. Conclusion. We are now capable of showing formula (1.1) of the introduction. We begin with a result giving a lower bound on the number of pairings, which will enable us to show that the dimension of the hypergeometric varieties is always $\leq n-4$.

PROPOSITION 5.9. Let \underline{s} be distinct from the class of (0, 1, ..., n-1) and of (0, ..., 0) and let s be a representative of \underline{s} . We can choose sequences $(v_1, ..., v_m)$ and $(w_1, ..., w_m)$ satisfying the assumptions of Remark 5.5 such that we have the pairing

$$\forall i \in [1; (2m - n + 1)/2], \quad w_{2i-1} - v_{2i-1} \equiv -(w_{2i} - v_{2i}) \bmod n.$$

Proof. Let (v_1, \ldots, v_m) and (w_1, \ldots, w_m) be as in Remark 5.5. By Theorem 1.2 of [1, p. 126], it is possible to permute (w_1, \ldots, w_m) so that the $v_i - w_i$ are pairwise distinct. Define V to be the subset $\{v_i - w_i\}$ of $\mathbb{Z}/n\mathbb{Z}$ (it has m elements) and μ to be the number of opposite pairs contained in V. Then

$$2\mu = |V \cap (-V)| = 2m - |V \cup (-V)| \ge 2m - (n-1).$$

As 2μ is the maximal number of pairings, this ends the proof. \blacksquare

Theorem 5.10. If $\psi^n \neq 1$, we can write

$$|X_{\psi}(\mathbb{F}_q)| = 1 + q + \dots + q^{n-2} + N_{\text{mirror}} + q^{(n-3)/2}N_1 + q^{(n-5)/2}N_3 + \dots + qN_{n-4},$$

where each N_d is a sum of terms of the form $|H_{\lambda}(\mathbb{F}_q)| - (q-1)^{l-1}q^{d+1-l}$ where α_i and β_j are obtained from each \underline{s} as described in §5.3 and where each $H_{\lambda} \subset \mathbb{A}^{d+2}$ is a variety of hypergeometric type of odd dimension equal to d with $1 \le d \le n-4$ (here, $\lambda = 1/\psi^n$) as considered in §3.1.

Proof. We saw in Theorem 4.10 that if $\psi \neq 0$ and $q \equiv 1 \mod n$, we could write

$$|X_{\psi}(\mathbb{F}_q)| = 1 + q + \dots + q^{n-2} + N_{\underline{0}} + \sum_{\underline{s} \neq \underline{0}} N_{\underline{s}}.$$

In Theorem 4.12, we recalled Wan's result that $N_{\underline{0}} = N_{\text{mirror}}$ and in Lemma 4.13, we showed that the term corresponding to $(0, 1, \dots, n-1)$ was zero when $\psi^n \neq 1$.

Now consider \underline{s} distinct from the class of $(0, \ldots, 0)$ and of $(0, 1, \ldots, n-1)$. Let m' be the greatest even integer $\leq m-2$ such that there exist (v_1, \ldots, v_m) and (w_1, \ldots, w_m) as in Remark 5.5 satisfying

$$\forall i \in [1; m'/2], \quad w_{2i-1} - v_{2i-1} \equiv -(w_{2i} - v_{2i}) \bmod n.$$

By Proposition 5.9, we have $m' \geq 2m - n + 1$ (note that, by Remark 5.3(d), $m+3 \leq n$, hence $m-2 \geq 2m-n+1$). The dimension d=2m-m'-3 of the corresponding variety of hypergeometric type considered in Theorem 5.7 thus satisfies $1 \leq d \leq n-4$.

Moreover, we have $q^{(n+1)/2-(2m-m')/2}=q^{(n-d-2)/2}$, and so, as d varies between 1 and n-4, these powers of q take the values $q^{(n-3)/2},\ldots,q$ respectively and all these values are obtained; indeed, if we consider an integer m such that $2 \leq m = d+1 \leq n-3$ and define $s = \left(0,\ldots,0,1,n-1,2,n-2,\ldots,\frac{n-m-1}{2},n-\frac{n-m-1}{2}\right)$, then $w=\left(0,\ldots,0\right)$ and $v=\left(\frac{n-m+1}{2},n-\frac{n-m+1}{2},\ldots,\frac{n-1}{2},\frac{n+1}{2}\right)$ each consist of m elements and we have m'=m-2 with the notations of Theorem 5.7. \blacksquare

6. Examples. To illustrate the methods just presented, let us detail explicitly the cases n = 5 and n = 7; these examples are given in terms of the hypersurfaces of hypergeometric type from §3.2.

EXAMPLE 6.1 (n=5). Let us recover the results announced by Candelas, de la Ossa and Rodríguez-Villegas in [4] in the non-singular and non-diagonal case (see [5] for a complete treatment of the n=5 case). We are interested in the factorisation of the zeta function of the quintic $\mathcal{M}_{\psi} \colon x_1^5 + \dots + x_5^5 - 5\psi x_1 \dots x_5 = 0$ when $\psi \neq 0$ and $\psi^5 \neq 1$. We list all the

classes $(s_1, ..., s_5) \neq (0, 0, 0, 0, 0)$, (0, 1, 2, 3, 4) (following the notations from §§4.1, 5.1, 5.2 and 5.3):

<u>s</u>	γ_s	K_s	m	m'	\overline{d}
(0,0,0,1,4)	20	2	2	0	1
(0,0,1,1,3)	30	2	2	0	1

Using the method described above, we obtain the following table (the hypergeometric hypersurfaces are all of the form $y^5 = x^{v_1}(1-x)^{v_2}(1-\frac{1}{v^5}x)^{5-v_2}$).

<u>s</u>	v_1	v_2	w_1	w_2	Equation
(0,0,0,1,4)	2	3	0	0	$y^5 = x^2 (1-x)^3 (1 - \frac{1}{\psi^5}x)^2$
(0,0,1,1,3)	2	4	0	1	$y^5 = x^2 (1 - x)^4 (1 - \frac{1}{\psi^5} x)$

We find the same equations as those given in $[4, \S 11.1]$:

$$\mathcal{A}_{\psi} \colon y^{5} = x^{2} (1 - x)^{3} \left(1 - \frac{1}{\psi^{5}} x \right)^{2},$$
$$\mathcal{B}_{\psi} \colon y^{5} = x^{2} (1 - x)^{4} \left(1 - \frac{1}{\psi^{5}} x \right).$$

We set $N_{\mathcal{A}_{\psi}} = |\mathcal{A}_{\psi}(\mathbb{F}_q)| - q$ and $N_{\mathcal{B}_{\psi}} = |\mathcal{B}_{\psi}(\mathbb{F}_q)| - q$ (these are numbers of affine points). We have, when $\psi \neq 0$, $\psi^5 \neq 1$ and $q \equiv 1 \mod 5$,

$$|\mathcal{M}_{\psi}(\mathbb{F}_q)| = 1 + q + q^2 + q^3 + N_{\text{mirror}} + 10qN_{\mathcal{A}_{\eta_b}} + 15qN_{\mathcal{B}_{\eta_b}}.$$

EXAMPLE 6.2 (n=7). We use the preceding results to find the factorisation of the zeta function of the septic S_{ψ} : $x_1^7 + \cdots + x_7^7 - 7\psi x_1 \dots x_7 = 0$. We list the $(s_1, \dots, s_7) \neq (0, \dots, 0)$, (0, 1, 2, 3, 4, 5, 6) (following the notations from §§4.1, 5.1, 5.2 and 5.3):

<u>s</u>	γ_s	K_s	m	m'	d
(0,0,0,1,2,5,6)	840	2	2	0	1
(0,0,1,1,3,4,5)	1260	2	2	0	1
(0,0,1,1,2,4,6)	1260	2	2	0	1
$\overline{(0,0,0,0,1,2,4)}$	210	3	3	0	3
(0,0,0,1,1,2,3)	420	1	3	0	3
(0,0,1,1,3,3,6)	630	3	3	0	3
$\overline{(0,0,0,0,0,1,6)}$	42	2	4	2	3
(0,0,0,0,1,1,5)	105	1	4	2	3
(0,0,0,1,1,1,4)	140	2	4	2	3
(0,0,0,1,1,6,6)	210	2	4	2	3

The result is that, when $\psi \neq 0$, $\psi^7 \neq 1$ and $q \equiv 1 \mod 7$, the number of points takes the form

$$|S_{\psi}(\mathbb{F}_q)| = 1 + q + q^2 + q^3 + q^4 + q^5 + N_{\text{mirror}} + q^2 N_1 + q N_3,$$

where the terms corresponding to curves of \mathbb{A}^2 can be written as

$$N_1 = 420N_{c_1} + 630N_{c_2} + 630N_{c_3},$$

and those corresponding to threefold hypersurfaces of \mathbb{A}^4 can be written as

$$N_3 = 70N_{t_1} + 420N_{t_2} + 210N_{t_3} + 21N_{t_1'} + 105N_{t_2'} + 70N_{t_3'} + 105N_{t_4'},$$

where the various terms are defined in the following table (the corresponding points are counted in the affine space).

Equation of the hypersurface	Number of points
$y^7 = x^3 (1-x)^4 (1-\frac{1}{\psi^7}x)^3$	$q + N_{c_1}$
$y^7 = x^2 (1 - x)^6 (1 - \frac{1}{\psi^7} x)$	$q + N_{c_2}$
$y^7 = x^3 (1 - x)^5 (1 - \frac{1}{\psi^7} x)^2$	$q + N_{c_3}$
$\overline{y^7} = x_1^3 x_2^5 x_3^3 (1 - x_1)^4 (1 - x_2 - x_3)^6 (1 - \frac{1}{\psi^7} x_1 x_2)$	$q^3 + N_{t_1}$
$y^7 = x_1^4 x_2^5 x_3^4 (1 - x_1)^3 (1 - x_2 - x_3)^6 (1 - \frac{1}{\psi^7} x_1 x_2)$	$q^3 + N_{t_2}$
$y^7 = x_1^2 x_2^4 x_3^4 (1 - x_1)^6 (1 - x_2 - x_3)^5 (1 - \frac{1}{\psi^7} x_1 x_2)^2$	$q^3 + N_{t_3}$
$\overline{y^7} = x_1^2 x_2^5 x_3^3 (1 - x_1)^5 (1 - x_2)^2 (1 - x_3)^4 (1 - \frac{1}{\psi^7} x_1 x_2 x_3)^3$	$q^3 + N_{t_1'}$
$y^7 = x_1^3 x_2^3 x_3^2 (1 - x_1)^4 (1 - x_2)^4 (1 - x_3)^6 (1 - \frac{1}{\psi^7} x_1 x_2 x_3)$	$q^3 + N_{t_2'}$
$y^7 = x_1^3 x_2^5 x_3^2 (1 - x_1)^4 (1 - x_2)^3 (1 - x_3)^6 (1 - \frac{1}{\psi^7} x_1 x_2 x_3)$	$q^3 + N_{t_3'}$
$y^{7} = x_{1}^{3} x_{2}^{5} x_{3}^{2} (1 - x_{1})^{4} (1 - x_{2})^{3} (1 - x_{3})^{4} (1 - \frac{1}{\psi^{7}} x_{1} x_{2} x_{3})^{3}$	$q^3 + N_{t_4'}$

Let us justify for example the equation corresponding to [0,0,0,0,0,1,6]. We have $\{v_1,v_2,v_3,v_4\}=\{2,3,4,5\}$ and $w_1=w_2=w_3=w_4=0$. Take, for example, $v_1=2, v_2=5, v_3=3$ and $v_4=4$ so that $w_1-v_1=-(w_2-v_2)$ and $w_3-v_3=-(w_4-v_4)$. For this choice, we have m=4, m'=m-2=2 and the equation we obtain is

$$y^7 = x_1^2 x_2^5 x_3^3 (1 - x_1)^5 (1 - x_2)^2 (1 - x_3)^4 \left(1 - \frac{1}{\psi^7} x_1 x_2 x_3 \right)^3.$$

This is the equation corresponding to $N_{t'_1}$. The other equations follow in a similar way.

REMARK 6.3. Using the same method, we could treat the cases n = 11, n = 13, etc. The only difficulty is practical, as the number of classes (s_1, \ldots, s_n) grows quickly with n.

Acknowledgments. I would like to thank my thesis advisor, J. Oesterlé, for the numerous improvements he suggested concerning the text. I would also like to thank Surya Ramana for providing a reference concerning Proposition 5.9.

References

- [1] N. Alon, Additive Latin transversals, Israel J. Math. 117 (2000), 125–130.
- [2] B. Berndt, R. Evans and K. Williams, Gauss and Jacobi Sums, Willey, New York, 1998.
- [3] P. Candelas, X. de la Ossa and F. Rodríguez-Villegas, Calabi-Yau manifolds over finite fields, I, preprint, 2000, arXiv:hep-th/0012233v1.
- [4] —, —, —, Calabi-Yau manifolds over finite fields, II, in: Calabi-Yau Varieties and Mirror Symmetry, N. Yui et al. (eds.), Fields Inst. Comm. 38, Amer. Math. Soc., 2003, 121–157.
- [5] P. Goutet, On the zeta function of a family of quintics, J. Number Theory 130 (2010), 478–492.
- [6] C. D. Haessig, Equalities, congruences, and quotients of zeta functions in arithmetic mirror symmetry, in: Mirror Symmetry V, N. Yui et al. (eds.), AMS/IP Stud. Adv. Math. 38, Amer. Math. Soc., 2006, 178–183 (appendix to [10]).
- [7] N. Katz, Another look at the Dwork family, in: Algebra, Arithmetic and Geometry—Manin Festschrift, Y. Tschinkel (ed.), to appear; http://www.math.princeton.edu/~nmk/dworkfamilyfinal.pdf.
- [8] R. Kloosterman, The zeta-function of monomial deformations of Fermat hypersurfaces, Algebra Number Theory 1 (2007), 421–450.
- [9] N. Koblitz, The number of points on certain families of hypersurfaces over finite fields, Compos. Math. 48 (1983), 3–23.
- [10] D. Wan, Mirror symmetry for zeta functions, in: Mirror Symmetry V, N. Yui et al. (eds.), AMS/IP Stud. Adv. Math. 38, Amer. Math. Soc., 2006, 159–184.
- [11] A. Weil, Numbers of solutions of equations in finite fields, Bull. Amer. Math. Soc. 55 (1949), 497–508.

Philippe Goutet Institut de Mathématiques de Jussieu case 247, 4 place Jussieu 75252 Paris Cedex 05, France E-mail: goutet@math.jussieu.fr

Received on 2.9.2009 (6136)