TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 358, Number 11, November 2006, Pages 4935–4957
S 0002-9947(06)03859-1
Article electronically published on April 11, 2006

THE INVARIANT FACTORS OF THE INCIDENCE MATRICES OF POINTS AND SUBSPACES IN $\mathrm{PG}(n,q)$ AND $\mathrm{AG}(n,q)$

DAVID B. CHANDLER, PETER SIN, AND QING XIANG

ABSTRACT. We determine the Smith normal forms of the incidence matrices of points and projective $(r-1)$-dimensional subspaces of $\mathrm{PG}(n,q)$ and of the incidence matrices of points and r-dimensional affine subspaces of $\mathrm{AG}(n,q)$ for all n, r, and arbitrary prime power q.

1. INTRODUCTION

Let $\mathbb{F}_q$ be the finite field of order q, where $q = p^t$, p is a prime and t is a positive integer, and let V be an $(n+1)$-dimensional vector space over $\mathbb{F}_q$. We denote by $\mathrm{PG}(V)$ (or $\mathrm{PG}(n,q)$ if we do not want to emphasize the underlying vector space) the n-dimensional projective geometry of V. The elements of $\mathrm{PG}(V)$ are subspaces of V and two subspaces are considered to be incident if one is contained in the other. We call one-dimensional subspaces of V *points* of $\mathrm{PG}(V)$ and we call n-dimensional subspaces of V *hyperplanes* of $\mathrm{PG}(V)$. More generally, we regard r-dimensional subspaces of V as projective $(r-1)$-dimensional subspaces of $\mathrm{PG}(V)$. We will refer to r-dimensional subspaces of V as r-subspaces and denote the set of these spaces in V as $\mathcal{L}_r$. The set of projective points is then $\mathcal{L}_1$. In this paper, we are concerned with the incidence relation between $\mathcal{L}_r$ and $\mathcal{L}_1$. Specifically, let A be a (0,1)-matrix with rows indexed by elements Y of $\mathcal{L}_r$ and columns indexed by elements Z of $\mathcal{L}_1$, and with the (Y,Z) entry equal to 1 if and only if $Z \subset Y$. We are interested in finding the Smith normal form ([9], p. 279) of A.

The incidence matrix A has been studied at least since the 1960s. In fact, several authors have considered the more general incidence matrices $A_{r,s}$ of r-subspaces vs. s-subspaces, where s is not necessarily one. Most of their investigations were on the rank of $A_{r,s}$ over fields K of various characteristics. When $K = \mathbb{Q}$, Kantor in [15] showed that the matrix $A_{r,s}$ has full rank under certain natural conditions on r and s, and when $\mathrm{char}(K) = \ell$, where ℓ does not divide q, the rank of $A_{r,s}$ over K was given by Frumkin and Yakir [11]. The most interesting case is when $\mathrm{char}(K) = p$. In this case, the problem of finding the rank of $A_{r,s}$ is open in general (cf. [13]). However, under the additional condition $s = 1$, Hamada [14] gave a complete solution to the problem of finding the p-rank of A (known as Hamada's formula). In this paper, we are not only interested in the p-rank of A, but also the Smith normal form of A as an integral matrix. There are a couple of reasons for us to study this problem.

Received by the editors April 27, 2004 and, in revised form, September 27, 2004.
2000 *Mathematics Subject Classification.* Primary 05E20; Secondary 20G05, 20C11.
The second author was partially supported by NSF grant DMS-0071060. The third author was partially supported by NSA grant MDA904-01-1-0036.

First, if we use the elements of $\mathcal{L}_1$ as points and use the elements of $\mathcal{L}_r$ as blocks, then we obtain what is called a 2-design [2] with "classical parameters". It is known that there exist many 2-designs with classical parameters [5]. A standard way to distinguish nonisomorphic designs with the same parameters is by comparing the p-ranks of their incidence matrices. Unfortunately, nonisomorphic designs sometimes have the same p-rank. In such a situation, one can try to prove nonisomorphism of designs by comparing the Smith normal forms of the incidence matrices [8]. Therefore it is of interest to find Smith normal forms of incidence matrices of designs.

Second, let Ω be an n-set. We say that an r-subset of Ω is *incident* with an s-subset of Ω if one is contained in the other. In [22], Wilson found a diagonal form of the incidence matrix of r-subsets versus s-subsets of Ω. One can consider the q-analogue of this problem, namely, finding the Smith normal form of the incidence matrix $A_{r,s}$ defined above. So far we have only succeeded in solving this problem in the case where $s = 1$. As far as we know, the problem of finding the p-rank of $A_{r,s}$ is open, let alone finding the p-part of the Smith form of $A_{r,s}$. (We mention that the p'-part of the Smith normal form of $A_{r,s}$ is known. See [7].)

We briefly summarize previous work on or related to the problem of finding the Smith form of the incidence between $\mathcal{L}_1$ and $\mathcal{L}_r$. Hamada [14] determined the p-rank of the incidence between projective points and $(r-1)$-subspaces of $\mathrm{PG}(n,q)$ for any values of p, t, r, and n. The work of Hamada in [14] is based on an earlier paper of Smith [19]. A more conceptual proof of Hamada's formula, independent of [19], was given in [4]. Lander [16] found the Smith form for the incidence between points and lines in $\mathrm{PG}(2,q)$. Black and List [6] determined the invariant factors of the incidence between points and hyperplanes in the case where $q = p$ (i.e., $t = 1$). More recently, Liebler [17] and the second author each determined the invariant factors of the incidence between points and hyperplanes for general q. The invariant factors of the incidence between points and arbitrary r-spaces when $q = p$ (i.e., $t = 1$) were computed in [18]. Finally, Liebler and the second author [17] had conjectured formulas for the invariant factors of the incidence between points and arbitrary r-subspaces for general q, and could prove their formulas in the cases where $q = p$, p^2, or p^3. In this paper we use a combination of techniques from number theory and representation theory to confirm this conjecture.

In the following we will give a brief overview of the paper. For convenience, we define the map

$$\eta_{1,r} : \mathbb{Z}^{\mathcal{L}_1} \to \mathbb{Z}^{\mathcal{L}_r} \tag{1.1}$$

by letting $\eta_{1,r}(Z) = \sum_{Y \in \mathcal{L}_r, Z \subset Y} Y$ for every $Z \in \mathcal{L}_1$, and then extending $\eta_{1,r}$ linearly to $\mathbb{Z}^{\mathcal{L}_1}$. The matrix of $\eta_{1,r}$ with respect to the basis $\mathcal{L}_1$ of $\mathbb{Z}^{\mathcal{L}_1}$ and the basis $\mathcal{L}_r$ of $\mathbb{Z}^{\mathcal{L}_r}$ is exactly the matrix A defined above. We will use the same $\eta_{1,r}$ to denote the linear map from $R^{\mathcal{L}_1}$ to $R^{\mathcal{L}_r}$ defined in the same way as above, where R is a certain p-adic local ring with maximal ideal $\mathfrak{p}$ and residue field $\mathbb{F}_q$ (see details in Section 2). The paper is organized as follows. In Section 2, we introduce the monomial basis $\mathcal{M}$ of $\mathbb{F}_q^{\mathcal{L}_1}$ and its Teichmüller lifting to a basis $\mathcal{M}_R$ of $R^{\mathcal{L}_1}$. These bases are very important for finding the Smith normal form of A. In Section 3, we state our main theorem (Theorem 3.3) which gives the Smith normal form of A. We also include an elementary proof of a well-known fact stating that all the invariant factors of A are powers of p except the last one. In Section 4, we discuss

Wan's theorem [21] on p-adic estimates of certain multiplicative character sums. Wan's theorem can be applied directly to our situation to give lower bounds on the (p-adic) invariant factors of A (now viewed as a matrix with entries from R). In order to prove that these lower bounds indeed give the p-adic invariant factors of A, considerable effort is needed. In Section 5, we prove that there exists a basis $\mathcal{B}$ of $R^{\mathcal{L}_1}$ whose reduction modulo $\mathfrak{p}$ is the monomial basis of $\mathbb{F}_q^{\mathcal{L}_1}$ such that the matrix of $\eta_{1,r}$ with respect to $\mathcal{B}$ and some basis of $R^{\mathcal{L}_r}$ is the (p-adic) Smith normal form of A. Next we prove a refinement of this result in Section 6. We show that there exists a basis $\mathcal{B}$ of $R^{\mathcal{L}_1}$ with the following properties:

(1) $\mathcal{B}$ contains certain elements of $\mathcal{M}_R$—we will make this precise in Section 6;
(2) the reduction modulo $\mathfrak{p}$ of $\mathcal{B}$ is $\mathcal{M}$; and
(3) there exists a basis $\mathcal{C}$ of $R^{\mathcal{L}_r}$ such that the matrix of $\eta_{1,r}$ with respect to $\mathcal{B}$ and $\mathcal{C}$ is the p-adic Smith normal form of A.

The proof of this result uses the natural action of the general linear group on $R^{\mathcal{L}_1}$, Jacobi sums, and Stickelberger's theorem on Gauss sums. In Section 7, combining the results in previous sections, we give a proof of a more precise statement (Theorem 7.2) which implies our main theorem. Finally in Section 8, we use our results in the projective geometry case to obtain the Smith normal form of the incidence matrix of points and r-flats of $\mathrm{AG}(n,q)$.

2. Monomial bases

As we will see, most of the invariant factors of A are p-powers. It will be helpful to view the entries of A as coming from some p-adic local ring. Let $q = p^t$ and let $K = \mathbb{Q}_p(\xi_{q-1})$ be the unique unramified extension of degree t over $\mathbb{Q}_p$, the field of p-adic numbers, where ξ_{q-1} is a primitive $(q-1)^{\text{th}}$ root of unity in K. Let $R = \mathbb{Z}_p[\xi_{q-1}]$ be the ring of integers in K and let $\mathfrak{p}$ be the unique maximal ideal in R. Then R is a principal ideal domain, and the reduction of $R \pmod{\mathfrak{p}}$ will be $\mathbb{F}_q$. Define $\bar{x}$ to be $x \pmod{\mathfrak{p}}$ for $x \in R$. Let T_q be the set of roots of $x^q = x$ in R (a Teichmüller set) and let T be the Teichmüller character of $\mathbb{F}_q$, so that $T(\bar{x}) = x$ for $x \in T_q$. We will use T to lift a basis of $\mathbb{F}_q^{\mathcal{L}_1}$ to a basis of $R^{\mathcal{L}_1}$.

In (1.1), we defined the map $\eta_{1,r}$ from $\mathbb{Z}^{\mathcal{L}_1}$ to $\mathbb{Z}^{\mathcal{L}_r}$. Now we use the same $\eta_{1,r}$ to denote the map from $R^{\mathcal{L}_1}$ to $R^{\mathcal{L}_r}$ sending a 1-space to the formal sum of all r-spaces incident with it. The matrix A is then the matrix of $\eta_{1,r}$ with respect to the (standard) basis $\mathcal{L}_1$ of $R^{\mathcal{L}_1}$ and the (standard) basis $\mathcal{L}_r$ of $R^{\mathcal{L}_r}$. Crucial to our approach of finding the Smith form of A is what we call a monomial basis for $R^{\mathcal{L}_1}$. We introduce this basis below.

We start with the monomial basis of $\mathbb{F}_q^{\mathcal{L}_1}$. This basis was discussed in detail in [4]. Let $V = \mathbb{F}_q^{n+1}$. Then V has a standard basis $v_0, v_1, \ldots, v_n$, where

$$v_i = (\underbrace{0, 0, \ldots, 0, 1}_{i+1}, 0, \ldots, 0).$$

We regard $\mathbb{F}_q^V$ as the space of functions from V to $\mathbb{F}_q$. Any function $f \in \mathbb{F}_q^V$ can be given as a polynomial function of $n+1$ variables corresponding to the $n+1$ coordinate positions: write the vector $\mathbf{x} \in V$ as

$$\mathbf{x} = (x_0, x_1, \ldots, x_n) = \sum_{i=0}^{n} x_i v_i;$$

then $f = f(x_0, x_1, \ldots, x_n)$. The function x_i is, for example, the linear functional that projects a vector in V onto its i^{th} coordinate in the standard basis.

As a function on V, $x_i^q = x_i$, for each $i = 0, 1, \ldots, n$, so we obtain all the functions via the q^{n+1} monomial functions in

$$\left\{ \prod_{i=0}^{n} x_i^{b_i} \mid 0 \le b_i < q, i = 0, 1, \ldots, n \right\}. \tag{2.1}$$

Since the characteristic function of $\{0\}$ in V is $\prod_{i=0}^{n}(1 - x_i^{q-1})$, we obtain a basis for $\mathbb{F}_q^{V\setminus\{0\}}$ by excluding $x_0^{q-1}x_1^{q-1}\cdots x_n^{q-1}$ from the set in (2.1).

The functions on $V \setminus \{0\}$ which descend to $\mathcal{L}_1$ are exactly those which are invariant under scalar multiplication by $\mathbb{F}_q^*$. Therefore we obtain a basis $\mathcal{M}$ of $\mathbb{F}_q^{\mathcal{L}_1}$ as follows:

$$\mathcal{M} = \left\{ \prod_{i=0}^{n} x_i^{b_i} \mid 0 \le b_i < q, \sum_i b_i \equiv 0 \pmod{q-1}, \right.$$
$$\left. (b_0, b_1, \ldots, b_n) \ne (q-1, q-1, \ldots, q-1) \right\}.$$

This basis $\mathcal{M}$ will be called the *monomial basis* of $\mathbb{F}_q^{\mathcal{L}_1}$, and its elements will be called *basis monomials*.

Now we lift the function $x_i : V \to \mathbb{F}_q$ to a function $T(x_i) : V \to R$, where T is the Teichmüller character of $\mathbb{F}_q$. For $(a_0, a_1, \ldots, a_n) \in V$, we have

$$T(x_i)(a_0, a_1, \ldots, a_n) = T(a_i) \in R.$$

For each basis monomial $\prod_{i=0}^{n} x_i^{b_i}$, we define $T(\prod_{i=0}^{n} x_i^{b_i})$ similarly. We have the following lemma.

Lemma 2.1. *The elements in the set*

$$\mathcal{M}_R = \left\{ T\Big(\prod_{i=0}^{n} x_i^{b_i}\Big) \mid 0 \le b_i < q, \sum_i b_i \equiv 0 \pmod{q-1}, \right.$$
$$\left. (b_0, b_1, \ldots, b_n) \ne (q-1, q-1, \ldots, q-1) \right\}$$

form a basis of the free R-module $R^{\mathcal{L}_1}$.

Proof. To simplify notation, we use M to denote the free R-module $R^{\mathcal{L}_1}$, set $v = |\mathcal{L}_1|$, and enumerate the elements of $\mathcal{M}_R$ as $f_1, f_2, \ldots, f_v$. Since the images of the elements of $\mathcal{M}_R$ in the quotient $M/\mathfrak{p}M$ are exactly the elements in $\mathcal{M}$, which form a basis of $\mathbb{F}_q^{\mathcal{L}_1} \cong M/\mathfrak{p}M$ (as vector spaces over $\mathbb{F}_q$), by Nakayama's lemma [1], the elements in $\mathcal{M}_R$ generate M, and since their number equals $\operatorname{rank} M$, they form a basis. □

The basis $\mathcal{M}_R$ will be called the *monomial basis* of $R^{\mathcal{L}_1}$, and its elements are called *basis monomials*.

3. The main theorem

Let $q = p^t$, and let V be an $(n+1)$-dimensional space over $\mathbb{F}_q$. As before we use A to denote the $|\mathcal{L}_r| \times |\mathcal{L}_1|$ matrix of the linear map $\eta_{1,r} : \mathbb{Z}^{\mathcal{L}_1} \to \mathbb{Z}^{\mathcal{L}_r}$ with respect to the standard bases of $\mathbb{Z}^{\mathcal{L}_1}$ and $\mathbb{Z}^{\mathcal{L}_r}$. It is known that all invariant factors of A (as a matrix over $\mathbb{Z}$) are p-powers except the last one, which is also divisible by $(q^r - 1)/(q - 1)$. In [18], a proof was given using the structure of the permutation

module for $\mathrm{GL}(n+1,q)$ acting on $\mathcal{L}_1$ over fields of characteristic prime to p. We give an elementary proof of the result.

Theorem 3.1. *Let A be the matrix of the map $\eta_{1,r}$ with respect to the standard bases of $\mathbb{Z}^{\mathcal{L}_r}$ and $\mathbb{Z}^{\mathcal{L}_1}$, and let $v = |\mathcal{L}_1|$. The invariant factors of A are all p-powers except for the v^{th} invariant, which is a p-power times $(q^r-1)/(q-1)$.*

Proof. We first define $\eta_{r,1} : \mathbb{Z}^{\mathcal{L}_r} \to \mathbb{Z}^{\mathcal{L}_1}$ to be the linear map sending each element of $\mathcal{L}_r$ to the formal sum of all the 1-spaces incident with it. Then the matrix of $\eta_{r,1}$ with respect to the standard bases of $\mathbb{Z}^{\mathcal{L}_r}$ and $\mathbb{Z}^{\mathcal{L}_1}$ is $A^\top$. For the purpose of proving this theorem, it will be more convenient to work with $A^\top$.

We define

$$\epsilon : \mathbb{Z}^{\mathcal{L}_1} \to \mathbb{Z}$$

to be the map sending each element in $\mathcal{L}_1$ to 1. Clearly ϵ maps $\mathbb{Z}^{\mathcal{L}_1}$ onto $\mathbb{Z}$ and $\operatorname{Im}\eta_{r,1}$ onto $(\frac{q^r-1}{q-1})\,\mathbb{Z}$. Thus,

$$\mathbb{Z}^{\mathcal{L}_1}/(\operatorname{Ker}\epsilon + \operatorname{Im}\eta_{r,1}) \cong \mathbb{Z}/(\tfrac{q^r-1}{q-1})\,\mathbb{Z}.$$

To finish the proof, we are reduced to showing that $(\operatorname{Ker}\epsilon + \operatorname{Im}\eta_{r,1})/\operatorname{Im}\eta_{r,1}$ is a p-group. We show that if $x \in \operatorname{Ker}\epsilon$, then $q^{r-1}x \in \operatorname{Im}\eta_{r,1}$. Now $\operatorname{Ker}\epsilon$ is spanned by vectors of the form $u-w$, where u and w are vectors representing individual elements in $\mathcal{L}_1$, so it is enough to show that $q^{r-1}(u-w)$ is in $\operatorname{Im}\eta_{r,1}$. Let U be some $(r+1)$-subspace of V which contains both u and w. We define $\tilde{\eta}_{1,r}$ to be the linear map which maps a projective point to the formal sum of the r-subspaces, which contain the point and also are contained in U. Also define $\mathbf{j}_U$ to be the formal sum of all the projective points inside U. Then $\eta_{r,1}$ restricted to r-subspaces inside U and $\tilde{\eta}_{1,r}$ are simply the hyperplane-to-point and point-to-hyperplane maps for the space U. By standard formula from design theory we have

$$\eta_{r,1}(\tilde{\eta}_{1,r}(z)) = q^{r-1}z + \frac{q^{r-1}-1}{q-1}\mathbf{j}_U$$

for every $z \in \mathcal{L}_1$. Hence by setting $z = u$ and $z = w$ respectively, and subtracting the resulting equations, we get

$$\eta_{r,1}(\tilde{\eta}_{1,r}(u-w)) = q^{r-1}(u-w)$$

which is the desired result. □

In view of Theorem 3.1, in order to get the Smith normal form of A, we just need to view A as a matrix with entries from $\mathbb{Z}_p$, the ring of p-adic integers, and find its Smith normal form over $\mathbb{Z}_p$. This will be the approach we take in the rest of the paper. To state our main theorem, we need more notation.

Let $\mathcal{H}$ denote the set of t-tuples $\xi = (s_0, s_1, \ldots, s_{t-1})$ of integers satisfying (for $0 \le j \le t-1$) the following:

$$\begin{array}{ll} (1) & 1 \le s_j \le n, \\ (2) & 0 \le ps_{j+1} - s_j \le (p-1)(n+1), \end{array} \tag{3.1}$$

with the subscripts read modulo t. The set $\mathcal{H}$ was introduced in [14], and used in [4] to describe the module structure of $\mathbb{F}_q^{\mathcal{L}_1}$ under the natural action of $\mathrm{GL}(n+1,q)$.

For a nonconstant basis monomial

$$f(x_0, x_1, \ldots, x_n) = x_0^{b_0} \cdots x_n^{b_n}$$

in $\mathcal{M}$, we expand the exponents

$$b_i = a_{i,0} + pa_{i,1} + \cdots + p^{t-1}a_{i,t-1} \quad 0 \le a_{i,j} \le p-1,$$

and let

$$\lambda_j = a_{0,j} + \cdots + a_{n,j}. \tag{3.2}$$

Because the total degree $\sum_{i=0}^{n} b_i$ is divisible by $q-1$, there is a uniquely defined t-tuple $(s_0, \ldots, s_{t-1}) \in \mathcal{H}$ [4] such that

$$\lambda_j = ps_{j+1} - s_j.$$

Explicitly

$$s_j = \frac{1}{q-1} \sum_{i=0}^{n} \Big(\sum_{\ell=0}^{j-1} p^{\ell+t-j} a_{i,\ell} + \sum_{\ell=j}^{t-1} p^{\ell-j} a_{i,\ell} \Big). \tag{3.3}$$

One way of interpreting the numbers s_j is that the total degree of f^{p^i} is $s_{t-i}(q-1)$, when the exponent of each coordinate x_i is reduced to be no more than $q-1$ by the substitution $x_i^q = x_i$. We will say that f is of *type* $\xi = (s_0, s_1, \ldots, s_{t-1})$. Also we say that the corresponding basis monomial $T(f) \in \mathcal{M}_R$ is of *type* ξ. (Note that in [4] ξ is called *a tuple in* $\mathcal{H}$ and the term *type* is used for certain other t-tuples in bijection with $\mathcal{H}$. However, since we will not use the latter, there is no risk of confusion within this paper.)

Let d_i be the coefficient of x^i in the expansion of $(\sum_{k=0}^{p-1} x^k)^{n+1}$. Explicitly,

$$d_i = \sum_{j=0}^{\lfloor i/p \rfloor} (-1)^j \binom{n+1}{j} \binom{n+i-jp}{n}.$$

Lemma 3.2. *Let d_i and λ_j be defined as above. The number of basis monomials in both $\mathcal{M}$ and $\mathcal{M}_R$ of type $\xi = (s_0, s_1, \ldots, s_{t-1})$ is $\prod_{j=0}^{t-1} d_{\lambda_j}$.*

Proof. From (3.2) each λ_j is the sum of $n+1$ integers which can be anywhere from 0 to $p-1$. The number of such choices is the same as the coefficient of x^{λ_j} in $(\sum_{k=0}^{p-1} x^k)^{n+1}$. Counting the choices for each λ_j as j runs from 0 to $t-1$ we get $\prod_{j=0}^{t-1} d_{\lambda_j}$. □

We can now state the main theorem.

Theorem 3.3. *Let $\mathcal{L}_1$ be the set of projective points, let $\mathcal{L}_r$ be the set of projective $(r-1)$-spaces in $\mathrm{PG}(n,q)$, and let d_i and $\mathcal{H}$ be as above. For each t-tuple $\xi = (s_0, s_1, \ldots, s_{t-1}) \in \mathcal{H}$ let*

$$\lambda_i = ps_{i+1} - s_i$$

and let

$$d_\xi = \prod_{i=0}^{t-1} d_{\lambda_i}.$$

Then the p-adic invariant factors of the incidence matrix A between $\mathcal{L}_1$ and $\mathcal{L}_r$ are p^α, $0 \le \alpha \le (r-1)t$, with multiplicity

$$m_\alpha = \sum_{\xi \in \mathcal{H}_\alpha} d_\xi + \delta(0, \alpha),$$

where

$$\mathcal{H}_\alpha = \Big\{(s_0, s_1, \ldots, s_{t-1}) \in \mathcal{H} \mid \sum_{i=0}^{t-1} \max\{0, r - s_i\} = \alpha\Big\} \tag{3.4}$$

and

$$\delta(0,\alpha) = \begin{cases} 1, & \text{if } \alpha = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{3.5}$$

Remark 3.4. (1) The theorem was conjectured by Liebler and the second author [17].

(2) The multiplicity of 1 among the p-adic invariant factors, m_0, is exactly the p-rank of A, which was determined by Hamada; see [12, 4, 14]. The explicit formula is

$$m_0 = 1 + \sum_{(s_0,s_1,\ldots,s_{t-1})\in\mathcal{H}, s_i \geq r, \forall i} d_{(s_0,s_1,\ldots,s_{t-1})}.$$

(To match the above formula with the one in [4, p. 77], one notes that $d_{(s_0,\ldots,s_{t-1})} = d_{(n+1-s_0,\ldots,n+1-s_{t-1})}$ for each $(s_0, \ldots, s_{t-1}) \in \mathcal{H}$.)

(3) We also mention that the largest α of the exponents of the p-adic invariant factors of A is $(r-1)t$. It arises in the case where $\xi = (1, 1, \ldots, 1)$. From Theorem 3.3, we find that the multiplicity of $p^{(r-1)t}$ is

$$m_{(r-1)t} = d_{(1,1,\ldots,1)} = \binom{n+p-1}{n}^t,$$

which is one less than the p-rank of $\eta_{1,n}$.

We indicate how we proceed to prove Theorem 3.3. In order to get the Smith normal form of A over R, we will find two invertible matrices P and Q^{-1} with entries in R, such that

$$A = PDQ^{-1},$$

where D is an $|\mathcal{L}_r| \times |\mathcal{L}_1|$ diagonal matrix with p powers on its diagonal. The matrices Q and P will come from basis changes in $R^{\mathcal{L}_1}$ and $R^{\mathcal{L}_r}$, respectively.

Let $\{e_1, e_2, \ldots, e_v\}$, where $v = |\mathcal{L}_1|$, be the standard basis of $R^{\mathcal{L}_1}$, and let $\mathcal{M}_R = \{f_1, f_2, \ldots, f_v\}$ be the monomial basis of $R^{\mathcal{L}_1}$ constructed in Lemma 2.1. For $1 \leq j \leq v$, let $f_j = \sum_{i=1}^{v} q_{ij} e_i$, $q_{ij} \in R$, and let $Q = (q_{ij})$. Then

$$\eta_{1,r}(f_j) = \sum_{i=1}^{v} q_{ij} \eta_{1,r}(e_i).$$

Therefore the columns of AQ are the vectors $\eta_{1,r}(f_j)$, written with respect to the standard basis of $R^{\mathcal{L}_r}$. For $1 \leq j \leq v$, let p^{a_j} be the largest power of p dividing

every coordinate of $\eta_{1,r}(f_j)$. Then we try to factorize AQ as PD, where

$$D = \begin{pmatrix} p^{a_1} & 0 & 0 & \cdots & 0 \\ 0 & p^{a_2} & 0 & & \\ 0 & & \ddots & & \vdots \\ \vdots & & & p^{a_{v-1}} & 0 \\ 0 & & \cdots & 0 & p^{a_v} \\ 0 & & \cdots & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & \cdots & & 0 \end{pmatrix},$$

and P is an $|\mathcal{L}_r| \times |\mathcal{L}_r|$ matrix whose first v columns are $\frac{1}{p^{a_j}}\eta_{1,r}(f_j)$, $j = 1, 2, \ldots, v$. In order to get the Smith normal form of A, we need to have some information on a_j. For this purpose we need to have some lower bound on the p-adic valuations of the coordinates of $\eta_{1,r}(f_j)$. Let f_j be a typical basis monomial $T(x_0^{b_0}x_1^{b_1}\cdots x_n^{b_n})$ in $\mathcal{M}_R$, and let $Y \in \mathcal{L}_r$. Then the Y-coordinate of $\eta_{1,r}(f_j)$ is

$$\begin{aligned} \eta_{1,r}(f_j)(Y) &= \sum_{Z \subset Y, Z \in \mathcal{L}_1} f_j(Z) \\ &= \frac{1}{q-1} \sum_{\mathbf{x} \in \mathbb{F}_q^{n+1} \setminus \{(0,0,\ldots,0)\}, \mathbf{x} \in Y} T^{b_0}(x_0)T^{b_1}(x_1)\cdots T^{b_n}(x_n), \end{aligned}$$

where in the last summation $\mathbf{x} = (x_0, x_1, \ldots, x_n) \in \mathbb{F}_q^{n+1}$. Therefore the coordinates of $\eta_{1,r}(f_j)$ are all multiplicative character sums. Thanks to a theorem of Wan [21], one can indeed obtain lower bounds on the p-adic valuations of these multiplicative character sums. We discuss Wan's theorem and its applications in the next section.

4. Wan's theorem

We adopt the same notation as in Section 2. That is, $q = p^t$, $K = \mathbb{Q}_p(\xi_{q-1})$ is the unique unramified extension of degree t over $\mathbb{Q}_p$, $R = \mathbb{Z}_p[\xi_{q-1}]$ is the ring of integers in K, and $\mathfrak{p}$ is the unique maximal ideal in R. Define $\bar{x}$ to be $x \pmod{\mathfrak{p}}$ for $x \in R$. Let T_q be the set of roots of $x^q = x$ in R and let T be the Teichmüller character of $\mathbb{F}_q$, so that $T(\bar{x}) = x$ for $x \in T_q$. Then T is a p-adic multiplicative character of $\mathbb{F}_q$ of order $(q-1)$ and all multiplicative characters of $\mathbb{F}_q$ are powers of T. Following the convention of Ax [3], T^0 is the character that maps all elements of $\mathbb{F}_q$ to 1, while T^{q-1} maps 0 to 0 and all other elements to 1.

For $0 \le i \le n$ let $F_i(x_1, \ldots, x_r)$ be polynomials of degree d_i over $\mathbb{F}_q$ and let

$$\chi_i = T^{b_i} \quad (0 \le b_i \le q-1)$$

be multiplicative characters. We want the p-adic valuation $\nu_p(S_q(\chi, F))$ of the multiplicative character sum

$$S_q(\chi, F) = \sum_{\mathbf{x} \in \mathbb{F}_q^r} \chi_0(F_0(\mathbf{x}))\cdots\chi_n(F_n(\mathbf{x})).$$

For an integer $k \ge 0$ we define $\sigma_q(k)$ to be the sum of the digits in the expansion of k as a base q number and $\sigma(k)$ as the sum of the digits in the expansion of k as a base p number. Wan's Theorem ([21], Theorem 3.1) is the following.

Theorem 4.1 (Wan). *Let $d = \max_i d_i$ and $q = p^t$. Then the p-adic valuation of $S_q(\chi, F)$ is at least*

$$\sum_{\ell=0}^{t-1} \left\lceil \frac{r - \frac{1}{q-1}\sum_{i=0}^{n} \sigma_q(p^\ell b_i) d_i}{d} \right\rceil.$$

Here we state a slightly stronger version of the theorem, which follows immediately from the proof in [21].

Theorem 4.2.

$$\nu_p(S_q(\chi, F)) \geq \sum_{\ell=0}^{t-1} \max\left\{0, \left\lceil \frac{r - \frac{1}{q-1}\sum_{i=0}^{n} \sigma_q(p^\ell b_i) d_i}{d} \right\rceil\right\}.$$

We will use this theorem only in the case where each F_i is a linear homogeneous function. For the convenience of the reader we specialize the proof given in [21].

Theorem 4.3. *For each i, $0 \leq i \leq n$, let $\overline{F}_i(\bar{\mathbf{x}}) = \bar{\gamma}_{i1}\bar{x}_1 + \cdots + \bar{\gamma}_{ir}\bar{x}_r$ be a linear functional on $\mathbb{F}_q^r$, where $\bar{\gamma}_{ij} \in \mathbb{F}_q$ for all i, j. Then*

$$\nu_p(S_q(\chi, \overline{F})) \geq \sum_{\ell=0}^{t-1} \max\{0, r - \frac{1}{q-1}\sum_{i=0}^{n} \sigma_q(p^\ell b_i)\}.$$

Proof. We will write

$$F_i(\mathbf{x}) = \gamma_{i1}\, x_1 + \cdots + \gamma_{ir}\, x_r$$

to represent the lifted functions from T_q^r to R with $\gamma_{ij} = T(\bar{\gamma}_{ij})$. Using the congruence

$$T(\bar{x}) \equiv x^{q^r} \pmod{q^r}$$

for all $x \in R$, we get

$$S_q(\chi, \overline{F}) \equiv \sum_{\mathbf{x} \in T_q{}^r} \big(F_0(\mathbf{x})\big)^{b_0 q^r} \cdots \big(F_n(\mathbf{x})\big)^{b_n q^r} \pmod{q^r}. \tag{4.1}$$

Expanding (4.1) we get

$$S_q(\chi, \overline{F}) \tag{4.2}$$
$$\equiv \sum_{\substack{k_{i1}+\cdots+k_{ir}=b_i q^r \\ 0 \leq i \leq n}} \prod_{i=0}^{n} \binom{b_i q^r}{k_{i1}, \ldots, k_{ir}} \Big(\prod_{i=0}^{n}\prod_{j=1}^{r} \gamma_{ij}{}^{k_{ij}}\Big)\Big(\prod_{j=1}^{r}\sum_{x \in T_q} x^{\sum_i k_{ij}}\Big) \pmod{q^r}.$$

We use the formula of Legendre, $\nu_p(k!) = (k - \sigma(k))/(p-1)$, and get that the p-adic valuation of the multinomial coefficient part of (4.2) is

$$\frac{1}{p-1}\sum_{i=0}^{n}\Big(b_i q^r - \sigma(b_i) - \sum_{j=1}^{r}(k_{ij} - \sigma(k_{ij}))\Big) = \frac{1}{p-1}\sum_{i=0}^{n}\Big(\sum_{j=1}^{r}\sigma(k_{ij}) - \sigma(b_i)\Big). \tag{4.3}$$

For the Teichmüller set T_q we have

$$\sum_{x \in T_q} x^k = \begin{cases} 0, & \text{if } (q-1) \text{ does not divide } k, \\ q, & \text{if } k = 0, \\ q-1, & \text{if } (q-1) | k \text{ and } k > 0. \end{cases} \tag{4.4}$$

Therefore, in (4.2) we only need to consider those terms for which

$$\sum_{i=0}^{n} k_{ij} \equiv 0 \pmod{q-1} \tag{4.5}$$

for all $j = 1, 2, \ldots, r$. Since $k \equiv \sigma_q(k) \pmod{q-1}$, we see that (4.5) implies

$$\sum_{i=0}^{n} \sigma_q(k_{ij}) \equiv 0 \pmod{q-1}. \tag{4.6}$$

Given k_{ij} such that $\sum_{j=1}^{r} k_{ij} = b_i q^r$ for $0 \le i \le n$ and (4.5) is satisfied, assume that s coordinates of the vector

$$(\sum_{i=0}^{n} k_{i1}, \sum_{i=0}^{n} k_{i2}, \ldots, \sum_{i=0}^{n} k_{ir})$$

are not identically 0. Then the same is true for the corresponding entries of the vector

$$(\sum_{i=0}^{n} \sigma_q(k_{i1}), \sum_{i=0}^{n} \sigma_q(k_{i2}), \ldots, \sum_{i=0}^{n} \sigma_q(k_{ir})). \tag{4.7}$$

Summing up the entries of the vector in (4.7) we get

$$s(q-1) - \sum_{i=0}^{n} b_i \le \sum_{i=0}^{n} \Big(\sum_{j=1}^{r} \sigma_q(k_{ij}) - b_i \Big). \tag{4.8}$$

We note that for a nonnegative integer ℓ, (4.6) still holds with $\sigma_q(k_{ij})$ replaced by $\sigma_q(p^\ell k_{ij})$. Also $\sum_{i=0}^{n} \sigma_q(p^\ell k_{ij})$ is not identically 0 for the same s subscripts of j. Thus we have

$$s(q-1) - \sum_{i=0}^{n} \sigma_q(p^\ell b_i) \le \sum_{i=0}^{n} \Big(\sum_{j=1}^{r} \sigma_q(p^\ell k_{ij}) - \sigma_q(p^\ell b_i) \Big).$$

Noting that the right-hand side is nonnegative since $\sum_{j=1}^{r} k_{ij} = b_i q^r$, we sum over ℓ to get

$$\sum_{\ell=0}^{t-1} \max\{0, s(q-1) - \sum_{i=0}^{n} \sigma_q(p^\ell b_i)\} \le \frac{q-1}{p-1} \sum_{i=0}^{n} \Big(\sum_{j=1}^{r} \sigma(k_{ij}) - \sigma(b_i) \Big),$$

using the fact that

$$\sum_{\ell=0}^{t-1} \sigma_q(p^\ell k) = \frac{q-1}{p-1} \sigma(k).$$

Comparing with (4.3) we get that each term of (4.2) (with k_{ij} satisfying (4.5)) has p-adic valuation at least

$$t(r-s) + \sum_{\ell=0}^{t-1} \max\Big\{0, s - \frac{1}{q-1} \sum_{i=0}^{n} \sigma_q(p^\ell b_i)\Big\} \ge \sum_{\ell=0}^{t-1} \max\Big\{0, r - \frac{1}{q-1} \sum_{i=0}^{n} \sigma_q(p^\ell b_i)\Big\}.$$

This completes the proof. □

We now apply Wan's theorem to our situation. Let $f = T(x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n}) \in \mathcal{M}_R$ be a basis monomial. We use Theorem 4.3 to give a lower bound on the p-adic valuation of the coordinates of $\eta_{1,r}(f)$. Note that the coordinates of $\eta_{1,r}(f)$ are indexed by the r-spaces in $\mathcal{L}_r$. An r-subspace Y of $V = \mathbb{F}_q^{n+1}$ can be defined by a system of $(n+1-r)$ independent linear homogeneous equations. Putting the $n+1-r$ equations in reduced row echelon form, we have r coordinates which can run freely through $\mathbb{F}_q$ and the remaining $n+1-r$ coordinates are linear functions of those r coordinates. Without loss of generality we label the free coordinates

$(x_0, \ldots, x_{r-1}) = \mathbf{x}$ and express the defining equations of Y as $x_i = F_i(\mathbf{x})$ for $(r \le i \le n)$. The Y-coordinate of $\eta_{1,r}(f)$ is

(4.9)

$$\eta_{1,r}(f)(Y) = \frac{1}{q-1} \sum_{\mathbf{x} \in {\mathbb{F}_q}^r \setminus \{(0,0,\ldots,0)\}} T^{b_0}(x_0) \cdots T^{b_{r-1}}(x_{r-1}) T^{b_r}(F_r(\mathbf{x})) \cdots T^{b_n}(F_n(\mathbf{x})).$$

Lemma 4.4. *Let $f(x_0, \ldots, x_n) = T({x_0}^{b_0} \cdots {x_n}^{b_n})$ be a nonconstant basis monomial in $\mathcal{M}_R$. Then every coordinate of the image vector $\eta_{1,r}(f)$ is divisible by p^α with*

$$\alpha = \sum_{i=0}^{t-1} \max\{0, r - s_i\}, \tag{4.10}$$

where $(s_0, s_1, \ldots, s_{t-1})$ is the type of f as defined in (3.3).

Proof. Let Y be an arbitrary r-space in $\mathcal{L}_r$. By the above discussion, we may assume that Y is defined by $x_i = F_i(\mathbf{x})$, $i = r, r+1, \ldots, n$, where $\mathbf{x} = (x_0, x_1, \ldots, x_{r-1}) \in \mathbb{F}_q^r$. The Y-coordinate of $\eta_{1,r}(f)$ is then given by (4.9). By Theorem 4.3, we have

$$\nu_p(\eta_{1,r}(f)(Y)) \ge \sum_{\ell=0}^{t-1} \max\{0, r - \frac{1}{q-1} \sum_{i=0}^{n} \sigma_q(p^\ell b_i)\}.$$

Recalling that the type of f is denoted by $(s_0, s_1, \ldots, s_{t-1})$ and noting that $s_{t-\ell} = \frac{1}{q-1} \sum_{i=0}^{n} \sigma_q(p^\ell b_i)$ (reading s_t as s_0) for all $\ell = 0, 1, \ldots, t-1$, we have

$$\nu_p(\eta_{1,r}(f)(Y)) \ge \sum_{i=0}^{t-1} \max\{0, r - s_i\}.$$

This completes the proof. □

Let Q be the basis change matrix between the standard basis and the monomial basis $\mathcal{M}_R = \{f_1, f_2, \ldots, f_v\}$ of $R^{\mathcal{L}_1}$ (as used in Section 3). Using Lemma 4.4, we see that one can factorize AQ as PD, where

$$D = \begin{pmatrix} p^{\alpha_1} & 0 & 0 & \cdots & 0 \\ 0 & p^{\alpha_2} & 0 & & \\ 0 & & \ddots & & \vdots \\ \vdots & & & p^{\alpha_{v-1}} & 0 \\ 0 & & \cdots & 0 & p^{\alpha_v} \\ 0 & & \cdots & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & \cdots & & 0 \end{pmatrix},$$

p^{α_i} corresponds to the basis monomial $f_i \in \mathcal{M}_R$ of type $(s_0, s_1, \ldots, s_{t-1})$,

$$\alpha_i = \sum_{j=0}^{t-1} \max\{0, r - s_j\},$$

and P is an $|\mathcal{L}_r| \times |\mathcal{L}_r|$ matrix whose first v columns are $\frac{1}{p^{\alpha_i}} \eta_{1,r}(f_i)$, $i = 1, 2, \ldots, v$. We still need to show that D (with the diagonal entries suitably arranged) is indeed the Smith normal form of A.

5. p-filtrations and Smith normal form bases

Let $R = \mathbb{Z}_p[\xi_{q-1}]$ with maximal ideal $\mathfrak{p} = pR$ and residue field $\mathbb{F}_q$, and let $\eta_{1,r} : R^{\mathcal{L}_1} \to R^{\mathcal{L}_r}$ be the map defined before. In this section we prove that there exists a basis $\mathcal{B}$ of $R^{\mathcal{L}_1}$ whose reduction modulo $\mathfrak{p}$ is the monomial basis of $\mathbb{F}_q^{\mathcal{L}_1}$ such that the matrix of $\eta_{1,r}$ with respect to $\mathcal{B}$ and some basis of $R^{\mathcal{L}_r}$ is the Smith normal form of $\eta_{1,r}$. We begin with some general results on injective homomorphisms of free R-modules.

For any free R-module M we set $\overline{M} = M/\mathfrak{p}M$, and for any R-submodule L of M, let $\overline{L} = (L + \mathfrak{p}M)/\mathfrak{p}M$ be the image in $\overline{M}$.

Let $\phi : M \to N$ be an injective homomorphism of free R-modules of finite rank, with $\operatorname{rank} M = m \geq 1$.

Let

$$N' = \{x \in N \mid \exists j \geq 0, p^j x \in \operatorname{Im} \phi\}.$$

Then N' is the smallest R-module direct summand of N containing $\operatorname{Im} \phi$ (sometimes called its *purification*) and is also of rank m. The invariant factors of ϕ stay the same if we change the codomain to N'. This will often allow us to reduce to the case $\operatorname{rank} N = m$.

Define

$$M_i = \{m \in M \mid \phi(m) \in p^i N\}, \quad i = 0, 1, ...$$

Then we have a filtration

$$M = M_0 \supseteq M_1 \supseteq \cdots$$

of M and the filtration

$$\overline{M} = \overline{M}_0 \supseteq \overline{M}_1 \supseteq \cdots$$

of $\overline{M}$.

Since ϕ is injective and $N'/\operatorname{Im} \phi$ has finite exponent, it follows that there exists a smallest index ℓ such that $\overline{M}_\ell = 0$. So we have a finite filtration

$$\overline{M} = \overline{M}_0 \supseteq \overline{M}_1 \supseteq \cdots \supseteq \overline{M}_\ell = \{0\}.$$

Note that the inclusions need not be strict, though the last one is, by minimality of ℓ.

Proposition 5.1. *For $0 \leq i \leq \ell - 1$, p^i is an invariant factor of ϕ with multiplicity* $\dim(\overline{M}_i/\overline{M}_{i+1})$.

Proof. The theory of modules over PIDs says that there are bases of M and N' such that ϕ is represented by an $m \times m$ diagonal matrix whose entries are the invariant factors of ϕ. From this matrix we see that the multiplicity of p^i is $\dim(\overline{M}_i/\overline{M}_{i+1})$. □

Let us start with a basis $\overline{\mathcal{B}}_{\ell-1}$ of $\overline{M}_{\ell-1}$ and extend it to a basis of $\overline{M}_{\ell-2}$ by adding a set $\overline{\mathcal{B}}_{\ell-2}$ of vectors and so on until we have a basis

$$\overline{\mathcal{B}} = \overline{\mathcal{B}}_0 \cup \overline{\mathcal{B}}_1 \cup \cdots \cup \overline{\mathcal{B}}_{\ell-1}$$

of $\overline{M}$. At each stage we also select a set $\mathcal{B}_i \subset M_i$ of preimages of $\overline{\mathcal{B}}_i$ and expand the sets in the same way. The resulting set $\mathcal{B} = \bigcup_{i=0}^{\ell-1} \mathcal{B}_i$ is a basis of M, by Nakayama's lemma.

We show that this basis can be used to compute the Smith normal form of ϕ, namely that there is a basis $\mathcal{C}$ of N such that the matrix of ϕ with respect to $\mathcal{B}$ and $\mathcal{C}$ is the Smith normal form.

Now for e in $\mathcal{B}_i$, we have $p^i \parallel \phi(e)$, so $y = \frac{1}{p^i}\phi(e)$ is an element of N'. The elements y thus obtained from all elements of $\mathcal{B}$ are linearly independent elements of N', since ϕ is injective. Moreover, the index of $\operatorname{Im}\phi$ in the R-submodule of N' generated by these elements y is equal to the index of $\operatorname{Im}\phi$ in N' by the proposition. Therefore, these elements y form a basis of N'. The matrix of ϕ with respect to $\mathcal{B}$ and any basis of N obtained by extending this basis will then be in Smith normal form.

For convenience, we introduce a special name for bases such as $\mathcal{B}$ above.

Definition 5.2. We will call a basis $\mathcal{B}$ of M an *SNF basis of M for ϕ* if $\mathcal{B} = \bigcup_{i=0}^{\ell-1} \mathcal{B}_i$, where for each i we have $\mathcal{B}_i \subseteq M_i$ and $\mathcal{B}_i$ maps bijectively to a basis of $\overline{M}_i/\overline{M}_{i+1}$ under the composite map $M_i \to \overline{M}_i \to \overline{M}_i/\overline{M}_{i+1}$.

We now apply the above general theory to our situation. We will look at the case where $M = R^{\mathcal{L}_1}$, $N = R^{\mathcal{L}_r}$, $\phi = \eta_{1,r}$. Let $G = \mathrm{GL}(n+1, q)$. Then G acts on $\mathcal{L}_1$ and $\mathcal{L}_r$ and the map $\eta_{1,r}$ is an injective homomorphism of RG-modules, so the M_i are RG-modules and the $\overline{M}_i$ are $\mathbb{F}_q G$-modules.

We will use the following special properties of the $\mathbb{F}_q G$-module $\mathbb{F}_q^{\mathcal{L}_1}$.

Proposition 5.3. (1) *Two basis monomials of the same type generate the same $\mathbb{F}_q G$-submodule of $\mathbb{F}_q^{\mathcal{L}_1}$.*

(2) *Every $\mathbb{F}_q G$-submodule of $\mathbb{F}_q^{\mathcal{L}_1}$ has a basis consisting of all basis monomials in the submodule.*

Proof. Part (1) is immediate from [4, Theorem B]. (The field in [4] is taken to be an algebraically closed field k, not $\mathbb{F}_q$, but it follows from [4, Theorem A] that in fact all the kG-submodules of $k^{\mathcal{L}_1}$ are simply scalar extensions of $\mathbb{F}_q G$-submodules of $\mathbb{F}_q^{\mathcal{L}_1}$, so for example [4, Theorems A, B] also hold over $\mathbb{F}_q$.) Let S be an $\mathbb{F}_q G$-submodule of $\mathbb{F}_q^{\mathcal{L}_1}$ and let $\mathcal{K} \subseteq \mathcal{H} \cup \{(0, \ldots, 0)\}$ be the set of tuples of the composition factors of S. Let S' be the $\mathbb{F}_q G$-submodule generated by all basis monomials with tuples in $\mathcal{K}$. By [4, Theorem B], S' is the smallest $\mathbb{F}_q G$-submodule such that the set of tuples of its composition factors contains $\mathcal{K}$, so $S' = S$. Hence, by [4, Theorem B], in the expression of any element of S as a linear combination of basis monomials, only basis monomials with tuples in $\mathcal{K}$ occur, proving (2). □

Corollary 5.4. *$R^{\mathcal{L}_1}$ has an SNF basis for $\eta_{1,r}$ whose image in $\mathbb{F}_q^{\mathcal{L}_1}$ is the monomial basis.*

Proof. By Proposition 5.3(2) we can choose $\overline{\mathcal{B}}_i$ in the construction above to be the set of monomials in $\overline{M}_i$ which are not in $\overline{M}_{i+1}$. □

Whenever we have a basis $\mathcal{B}$ of $R^{\mathcal{L}_1}$ whose reduction modulo $\mathfrak{p}$ is the monomial basis, the type of an element of $\mathcal{B}$ will always mean the type of its image in the monomial basis.

Corollary 5.5. *Let $\mathcal{B}$ be an SNF basis of $R^{\mathcal{L}_1}$ for $\eta_{1,r}$ whose image in $\mathbb{F}_q^{\mathcal{L}_1}$ is the monomial basis. Then the invariants corresponding to two elements of $\mathcal{B}$ of the same type are equal.*

Proof. Let e, $f \in \mathcal{B}$ be two such basis elements, with images $\overline{e}$ and $\overline{f}$. Then

$$\begin{aligned} e \in M_j &\iff \overline{e} \in \overline{M}_j \quad \text{(def. of SNF basis)} \\ &\iff \overline{f} \in \overline{M}_j \quad \text{(Proposition 5.3(1))} \\ &\iff f \in M_j \quad \text{(def. of SNF basis).} \end{aligned}$$

□

6. Jacobi sums and the action of the general linear group on $R^{\mathcal{L}_1}$

In this section we will prove a refinement of Corollary 5.4 (see Lemma 6.5 for details). In order to prove this refinement, we need to use Jacobi sums and the action of the general linear group on $R^{\mathcal{L}_1}$. We first define Jacobi sums.

Let T be the Teichmüller character of $\mathbb{F}_q$ defined in Section 2, where $q = p^t$. We know that T is a p-adic multiplicative character of $\mathbb{F}_q$ of order $(q-1)$, and all multiplicative characters of $\mathbb{F}_q$ are powers of T. Again we adopt the convention that T^0 is the character that maps all elements of $\mathbb{F}_q$ to 1, while T^{q-1} maps 0 to 0 and all other elements to 1.

For any two integers b_0 and b_1, we define

$$J(T^{b_0}, T^{b_1}) = \sum_{x \in \mathbb{F}_q} T^{b_0}(x) T^{b_1}(1-x). \tag{6.1}$$

From the above definition and our convention on T^0 and T^{q-1}, we see that if $b_0 \not\equiv 0 \pmod{q-1}$, then

$$J(T^{b_0}, T^0) = 0 \text{ and } J(T^{b_0}, T^{q-1}) = -1.$$

Also we have $J(T^{-1}, T) = 1$. The Jacobi sum $J(T^{b_0}, T^{b_1})$ lies in $R = \mathbb{Z}_p[\xi_{q-1}]$. Naturally we want to know its p-adic valuation. Using Stickelberger's theorem on Gauss sums [20] (see [10] for further reference) and the well-known relation between Gauss and Jacobi sums, we have

Theorem 6.1. *Let b_0 and b_1 be integers such that $b_i \not\equiv 0 \pmod{q-1}$, $i = 0, 1$, and $b_0 + b_1 \not\equiv 0 \pmod{q-1}$. For any integer b, we use $\sigma(b)$ to denote the sum of digits in the expansion of the least nonnegative residue of b modulo $(q-1)$ as a base p number. Then*

$$\nu_p(J(T^{-b_0}, T^{-b_1})) = \frac{\sigma(b_0) + \sigma(b_1) - \sigma(b_0 + b_1)}{p-1}.$$

In other words, the number of times that p divides $J(T^{-b_0}, T^{-b_1})$ is equal to the number of carries in the addition $b_0 + b_1 \pmod{q-1}$.

We will now construct an element of RG with certain special properties. For this purpose, we will first describe the action of G on $R^{\mathcal{L}_1}$. We think of elements of $\mathcal{L}_1$ in homogeneous coordinates as row vectors and elements of G as matrices acting by right multiplication. Then $R^{\mathcal{L}_1}$ is the left RG-module given in the following way. For each function $f \in R^{\mathcal{L}_1}$ and $g \in G$, the function gf is given by

$$(gf)(Z) = f(Zg), \qquad Z \in \mathcal{L}_1.$$

Let $f_i = T(x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n}) \in \mathcal{M}_R$ be an arbitrary basis monomial. Let $\xi = \xi_{q-1}$ be a primitive $(q-1)^{\text{th}}$ root of unity in the Teichmüller set $T_q \subset R$, and let $\bar{\xi}$ be

its reduction modulo p. We define $g_\ell \in G$ to be the element which replaces x_0 by $x_0 + \bar{\xi}^\ell x_1$ and leaves all other x_i unchanged. Then

$$g_\ell f_i = T\big((x_0 + \bar{\xi}^\ell x_1)^{b_0} x_1^{b_1} \cdots x_n^{b_n}\big).$$

Let $g = \sum_{\ell=0}^{q-2} \xi^{-\ell} g_\ell \in RG$. The following lemma gives us gf_i.

Lemma 6.2. *Let f_i and g be as given. Then*

$$gf_i = \begin{cases} 0, & \text{if } b_0 = 0, \\ T(x_0^{q-2} x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}), & \text{if } b_0 = q-1, \\ \big(q(1 - T(x_0^{q-1})) - 1\big) T(x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}), & \text{if } b_0 = 1, \\ -J(T^{-1}, T^{b_0}) T(x_0^{b_0-1} x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}), & \text{otherwise.} \end{cases}$$

Proof. First note that

$$\begin{aligned} J(T^{-1}, T^0) &= 0, \\ J(T^{-1}, T^{q-1}) &= -1, \end{aligned}$$

so the cases $b_0 = 0$ and $b_0 = q-1$ are really covered by the general case. Therefore we will only consider two cases.

Case 1. $b_0 \neq 1$. First assume that x_0 and x_1 are both nonzero. We have

$$gf_i = \sum_{\ell=0}^{q-2} \xi^{-\ell} g_\ell f_i \tag{6.2}$$

$$= T(x_1^{b_1} \cdots x_n^{b_n}) \sum_{\ell=0}^{q-2} T^{-1}(\bar{\xi}^\ell) T^{b_0}(x_0 + \bar{\xi}^\ell x_1) \tag{6.3}$$

$$= T(x_1^{b_1} \cdots x_n^{b_n}) \sum_{u \in \mathbb{F}_q} T^{-1}(-\frac{x_1 u}{x_0}) T^{b_0}\left(1 - (-\frac{x_1 u}{x_0})\right) T(-1) T(x_0^{b_0-1} x_1) \tag{6.4}$$

$$= -J(T^{-1}, T^{b_0}) T(x_0^{b_0-1} x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}). \tag{6.5}$$

If $x_1 = 0$ we verify directly that (6.3) and (6.5) are both zero, so the formula is still valid. If $x_0 = 0$, since $b_0 \neq 1$, we see that (6.5) is 0; and (6.3) is also 0, since a nontrivial (multiplicative) character summed over $\mathbb{F}_q$ is zero. Therefore the formula still holds.

Case 2. $b_0 = 1$. In this case

$$gf_i = T(x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}) \sum_{\ell=0}^{q-2} T(\bar{\xi}^{-\ell} x_0 + x_1).$$

If $x_0 = 0$, then $gf_i = (q-1) T(x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n})$. If $x_0 \neq 0$ but $x_1 = 0$, then clearly we have $gf_i = 0$. If $x_0 \neq 0$ and $x_1 \neq 0$, then using the same calculations as in the case $b_0 \neq 1$, we have

$$gf_i = -J(T^{-1}, T) T(x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}) = -T(x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}).$$

In summary, the formula for gf_i in this case is

$$\big(q(1 - T(x_0^{q-1})) - 1\big) T(x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}).$$

This completes the proof. □

Corollary 6.3. *Let $f_i = T(x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n}) \in \mathcal{M}_R$ be a basis monomial, and let $g(j) = \sum_{\ell=0}^{q-2} \xi^{-\ell} g_{\ell p^{-j}}$ be the j^{th} Frobenius analog of g in Lemma 6.2 above. Then*

$$g(j)f_i = \begin{cases} 0, & \text{if } b_0 = 0, \\ T(x_0^{q-1-p^j} x_1^{b_1+p^j} x_2^{b_2} \cdots x_n^{b_n}), & \text{if } b_0 = q-1, \\ \big(q(1-T(x_0^{q-1})) - 1\big) T(x_1^{b_1+p^j} x_2^{b_2} \cdots x_n^{b_n}), & \text{if } b_0 = p^j, \\ -J(T^{-p^j}, T^{b_0}) T(x_0^{b_0-p^j} x_1^{b_1+p^j} x_2^{b_2} \cdots x_n^{b_n}), & \text{otherwise.} \end{cases}$$

Proof. Let ρ denote the Frobenius automorphism of R, which maps an element of the Teichmüller set T_q to its p^{th} power, and let $\mathbf{y} = (y_0, \ldots, y_n) = (x_0^{p^j}, \ldots, x_n^{p^j})$. We can write $f_i(\mathbf{x}) = f_i^{\rho^{-j}}(\mathbf{y}) = T(y_0^{b_0 p^{-j}} \cdots y_n^{b_n p^{-j}})$. We observe that $g_{\ell p^{-j}}$ replaces y_0 by $y_0 + \bar{\xi}^{\ell} y_1$. Therefore we can apply the previous lemma to get

$$g(j) f_i^{\rho^{-j}}(\mathbf{y})$$
$$= \begin{cases} 0, & \text{if } b_0 = 0, \\ T(y_0^{q-2} y_1^{b_1 p^{-j}+1} y_2^{b_2 p^{-j}} \cdots y_n^{b_n p^{-j}}), & \text{if } b_0 = q-1, \\ \big(q(1-T(y_0^{q-1})) - 1\big) T(y_1^{b_1 p^{-j}+1} y_2^{b_2 p^{-j}} \cdots y_n^{b_n p^{-j}}), & \text{if } b_0 = p^j, \\ -J(T^{-1}, T^{b_0 p^{-j}}) T(y_0^{b_0 p^{-j}-1} y_1^{b_1 p^{-j}+1} y_2^{b_2 p^{-j}} \cdots y_n^{b_n p^{-j}}), & \text{otherwise.} \end{cases}$$

Substituting $\mathbf{x}$ back in and noting that $J(\chi^p, \psi^p) = J(\chi, \psi)$, we get the result. □

For each basis monomial in $\mathcal{M}_R$ with at least one exponent strictly between 0 and $q-1$, we want to construct an element of RG which acts as the identity on that basis monomial and annihilates all other members of $\mathcal{M}_R$.

Lemma 6.4. *Let $\mathcal{M}_R = \{f_1, f_2, \ldots, f_v\}$ be the monomial basis of $R^{\mathcal{L}_1}$. For each $f_i = T(x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n}) \in \mathcal{M}_R$ with some b_j strictly between 0 and $q-1$, there is an element $h_i \in RG$ with the following property. If*

$$f = c_1 f_1 + c_2 f_2 + \cdots + c_v f_v$$

is any element in $R^{\mathcal{L}_1}$, then

$$h_i f = c_i f_i.$$

Proof. We will construct the required h_i in two steps. Let H denote the subgroup of diagonal matrices of G. Then each basis monomial in $\mathcal{M}_R$ spans a rank one RH-submodule of $R^{\mathcal{L}_1}$, which is the direct sum of all such submodules. Two basis monomials $f_i = T(x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n})$ and $f_j = T(x_0^{b_0'} x_1^{b_1'} \cdots x_n^{b_n'})$ afford the same character of H if and only if $b_i \equiv b_i' \bmod q-1$ for $0 \le i \le n$.

Since the order of H is not divisible by p, the group ring RH contains, for each character χ of H, an idempotent element projecting onto the χ-isotypic component of $R^{\mathcal{L}_1}$, the span of all the basis monomials affording χ.

If none of the exponents of f_i is divisible by $q-1$, then no other basis monomials afford the same character as f_i and we can take h_i to be the above idempotent. Now suppose that some exponents of f_i are divisible by $q-1$. We proceed successively for each exponent of f_i which is either 0 or $q-1$. Without loss of generality, assume that f_i has $b_0 = q-1$. We construct an element $h \in RG$ which annihilates every basis monomial in $\mathcal{M}_R$ for which $b_0 = 0$ and acts as the identity on f_i. (If f_i instead has $b_0 = 0$, then the element we want is $1-h$.)

Without loss of generality we will take $b_1 = a_{1,t-1}p^{t-1} + \cdots + a_{1,0}$ to be an exponent lying strictly between 0 and $q-1$ with $0 < a_{1,j} < p-1$ for some j. Then

we take the element $h_1 = g(j) \in RG$ from Lemma 6.3 that shifts p^j from b_0 to b_1. We get

$$h_1 f_i = T(x_0^{q-1-p^j} x_1^{b_1+p^j} x_2^{b_2} \cdots x_n^{b_n}).$$

If e is any other basis monomial of the form $e = T(x_0^{q-1} x_1^{b_1} \cdots)$, then we similarly have

$$h_1 e = T(x_0^{q-1-p^j} x_1^{b_1+p^j} \cdots),$$

and if x_0 has exponent 0 in e then from Corollary 6.3, we have

$$h_1 e = 0.$$

Next we set $h_2 = g'(j) \in RG$ to be the analog of $g(j)$ but with the roles of x_0 and x_1 interchanged. Noting that here $b_1 + p^j \neq p^j$ (we assumed that $0 < b_1 < q-1$), we get

$$\begin{aligned} h_2 h_1 f_i &= -J(T^{-p^j}, T^{b_1+p^j}) f_i, \\ h_2 h_1 e &= -J(T^{-p^j}, T^{b_1+p^j}) e, \quad \text{if the exponent of } x_0 \text{ in } e \text{ is } q-1, \\ h_2 h_1 e &= 0 \quad \text{otherwise.} \end{aligned}$$

Since there is no carry in the sum $p^j + b_1$, the Jacobi sum $J(T^{-p^j}, T^{b_1+p^j})$ is a unit in R (cf. Theorem 6.1). Hence the element h of RG we want is $-\frac{1}{J(T^{-p^j}, T^{b_1+p^j})} h_2 h_1$.

We can repeat the above process for each exponent of f_i that is divisible by $q-1$. The product of all the elements we have constructed is the element $h_i \in RG$ which kills every basis monomial in $\mathcal{M}_R$ except f_i. □

We now prove the main result in this section.

Lemma 6.5. *Assume $q > 2$. There exists an SNF basis of $R^{\mathcal{L}_1}$ for $\eta_{1,r}$, whose reduction modulo $\mathfrak{p}$ is $\mathcal{M}$, and which contains all the basis monomials of $\mathcal{M}_R$ having at least one exponent lying strictly between 0 and $q-1$.*

Proof. By Corollary 5.4, there exists an SNF basis $\mathcal{B} = \bigcup_{j=0}^{\ell-1} \mathcal{B}_j$ of $R^{\mathcal{L}_1}$ for $\eta_{1,r}$ such that the reduction of $\mathcal{B}$ modulo $\mathfrak{p}$ is $\mathcal{M}$. Let $f \in \mathcal{B}$, and let the reduction of f modulo $\mathfrak{p}$ be

$$\overline{f} = x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n} \in \mathcal{M},$$

with some b_j satisfying $0 < b_j < q-1$. Let $\mathcal{M}_R = \{f_1, f_2, \ldots, f_v\}$ with $f_1 = T(x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n})$, where $v = |\mathcal{L}_1|$. We write

$$f = c_1 f_1 + c_2 f_2 + \cdots + c_v f_v, \ c_i \in R.$$

Since $\overline{f} = \overline{f_1}$, we see that $\overline{c_1} = 1$, hence c_1 is a unit in R. Since there is an exponent b_j lying strictly between 0 and $q-1$, by Lemma 6.4 we can find $h_1 \in RG$ such that $h_1 f = c_1 f_1$. In the notation of Definition 5.2 with $M = R^{\mathcal{L}_1}$, we see that if $f \in \mathcal{B}_j$, then $f_1 \in M_j$ since M_j is an RG-submodule, so $\mathcal{B}' = (\mathcal{B} \setminus \{f\}) \cup \{f_1\}$ is again an SNF basis of $R^{\mathcal{L}_1}$ for $\eta_{1,r}$. We can repeat this process for every element in $\mathcal{B}$ whose reduction modulo $\mathfrak{p}$ has one exponent strictly lying between 0 and $q-1$. At the end, we obtain the required SNF basis of $R^{\mathcal{L}_1}$ for $\eta_{1,r}$. □

We will use $\mathcal{M}'_R$ to denote the special SNF basis of $R^{\mathcal{L}_1}$ for $\eta_{1,r}$ produced by Lemma 6.5. Again *the type of $f \in \mathcal{M}'_R$* is defined to be that of $\overline{f} \in \mathcal{M}$.

Lemma 6.6. *The invariants of $\eta_{1,r}$ corresponding to two elements of $\mathcal{M}'_R$ of types $(s_0, \ldots, s_{t-1})$ and $(s_1, s_2, \ldots, s_{t-1}, s_0)$, respectively, are equal.*

Proof. We may assume $t \geq 2$ since there is nothing to prove otherwise. For any type $\xi \in \mathcal{H}$, we can always find a basis monomial $f \in \mathcal{M}_R$ of type ξ and with at least one exponent lying strictly between 0 and $q-1$; hence $f \in \mathcal{M}'_R$. By Corollary 5.5, the invariants of $\eta_{1,r}$ corresponding to two elements in $\mathcal{M}'_R$ of the same type are equal. Therefore we may assume that the two elements of $\mathcal{M}'_R$ in the statement of the lemma are actually in $\mathcal{M}_R$.

The Frobenius field automorphism

$$\begin{aligned} \rho : \mathbb{F}_q &\to \mathbb{F}_q, \\ x_i &\mapsto x_i^p \end{aligned}$$

applied to the coordinates of V is an automorphism of the projective geometry. It maps points to points, subspaces to subspaces, and preserves incidence . The image of a point $Z = (x_0, \ldots, x_n)$ is $Z^\rho = (x_0^p, \ldots, x_n^p)$, and for an r-subspace Y, Y^ρ is the r-subspace containing the images of all the points incident with Y. Given a monomial function $f_i = T(x_0^{b_0} \cdots x_n^{b_n})$ we have

$$f_i^\rho = T(x_0^{pb_0} \cdots x_n^{pb_n}).$$

Clearly if f_i is of type $(s_0, \ldots, s_{t-1})$, then f_i^ρ is of type $(s_{t-1}, s_0, \ldots, s_{t-2})$ because λ_j becomes λ_{j+1} in (3.2). It is also clear that

$$f_i(Z^\rho) = f_i^\rho(Z)$$

so that

$$\eta_{1,r}(f_i)(Y^\rho) = \eta_{1,r}(f_i^\rho)(Y).$$

As Y runs through $R^{\mathcal{L}_r}$, so does Y^ρ. Thus, the coordinates of $\eta_{1,r}(f_i)$ are the same as the coordinates of $\eta_{1,r}(f_i{}^\rho)$ but permuted by ρ, so the invariants corresponding to f_i and f_i^ρ are equal. □

7. The proof of Theorem 3.3

Our aim in this section is to prove Theorem 3.3, and we will achieve this by proving the more detailed result of Theorem 7.2 below. Our proof depends on Lemma 4.4, which gives lower bounds on the p-adic valuations of the coordinates of $\eta_{1,r}(f)$, where $f \in \mathcal{M}_R$, and the results in Section 5 and 6.

We first prove a lemma.

Lemma 7.1. *Let f be a nonconstant basis monomial in $\mathcal{M}_R$. Then p does not divide $\eta_{1,r}(f)$ if and only if f has type $(s_0, s_1, \ldots, s_{t-1})$, with $s_j \geq r$ for all $0 \leq j \leq t-1$.*

Proof. Let $\overline{f}$ be the image modulo $\mathfrak{p}$ of f. Then p does not divide $\eta_{1,r}(f)$ if and only if the image of $\overline{f}$ under the induced map $\overline{\eta}_{1,r} : \mathbb{F}_q^{\mathcal{L}_1} \to \mathbb{F}_q^{\mathcal{L}_r}$ is nonzero. Suppose that $s_j < r$ for some j. By Lemma 4.4, $p | \eta_{1,r}(f)$. That is, only those basis monomials $\overline{f}$ of type $(s_0, s_1, \ldots, s_{t-1})$, where $s_j \geq r$ for all $0 \leq j \leq t-1$, could possibly have nonzero image under $\overline{\eta}_{1,r}$. On the other hand, by Hamada's formula, the rank of $\overline{\eta}_{1,r}$ is equal to one plus the number of $\overline{f}$'s with this property. Therefore, the images of all such basis monomials must be linearly independent, in particular, nonzero. Hence $p \nmid \eta_{1,r}(f)$ if and only if f has type $(s_0, s_1, \ldots, s_{t-1})$, where $s_j \geq r$ for all $0 \leq j \leq t-1$. This completes the proof. □

Theorem 7.2. *Let $\mathcal{M}'_R = \{f'_1, f'_2, \dots, f'_v\}$ with $\bar{f}'_1 = 1 \in \mathcal{M}$. Let the type of f'_i, $2 \le i \le v$, be $(s_0^{(i)}, s_1^{(i)}, \dots, s_{t-1}^{(i)})$ and let p^{β_i} be the invariant of $\eta_{1,r}$ corresponding to f'_i. Then*

$$\beta_i = \sum_{j=0}^{t-1} \max\{0, r - s_j^{(i)}\}.$$

Proof. We shall assume that $t \ge 2$. When $t = 1$ a similar and easier argument works, but we omit the details to keep the notation simple and the argument clear, since this case is already known [18]. Let $\alpha_i = \sum_{j=0}^{t-1} \max\{0, r - s_j^{(i)}\}$ and let $f_i \in \mathcal{M}_R$ be the basis monomial which has the same reduction modulo $\mathfrak{p}$ as f'_i, namely $f_i = T(\bar{f}'_i)$. We use the notation of Definition 5.2 with $M = R^{\mathcal{L}_1}$ and $\phi = \eta_{1,r}$. By Lemma 4.4, we have $f_i \in M_{\alpha_i}$. Since the image of $\bar{f}_i = \bar{f}'_i$ in $\overline{M}_{\beta_i}/\overline{M}_{\beta_i+1}$ is not zero, it follows that $\alpha_i \le \beta_i$.

Suppose by way of contradiction that $\beta_k > \alpha_k$ for some k. Let

$$f_k = T(x_0^{b_0} x_1^{b_1} \cdots x_n^{b_n})$$

be of type $(s_0, s_1, \dots, s_{t-1})$ (here we suppressed the superscript (k) of s_j to keep the notation simple). Assume that we have picked k so that if $\alpha_j < \alpha_k$, then $\alpha_j = \beta_j$. By Lemma 6.6 we can assume for convenience that $s_1 = \min\{s_0, \dots, s_{t-1}\}$. We have

$$\lambda_0 = ps_1 - s_0 \le n(p-1)$$

with equality only if $s_0 = s_1 = \cdots = s_{t-1} = n$ and

$$\lambda_1 = ps_2 - s_1 \ge 1.$$

We note that the case $s_0 = s_1 = \cdots = s_{t-1} = n$ will not occur by our assumption that $\beta_k > \alpha_k$. The reason is as follows. If f_k has type $(s_0, s_1, \dots, s_{t-1}) = (n, n, \dots, n)$, by Lemma 7.1 we see that $p \nmid \eta_{1,r}(f_k)$. Since $\bar{f}'_k = \bar{f}_k$, we have $p \nmid \eta_{1,r}(f'_k)$. But the invariant corresponding to f'_k is p^{β_k}, and we assumed that $\beta_k > \alpha_k = 0$, so $p | \eta_{1,r}(f'_k)$, a contradiction.

By Corollary 5.5, basis vectors in $\mathcal{M}'_R$ of the same type correspond to the same invariant, so in the sum $\lambda_0 = \sum_{i=0}^n a_{i,0}$ we can assume that $a_{0,0} = 0$, and we can also assume that $a_{1,0} < p - 1$ since the case $s_0 = s_1 = \cdots = s_{t-1} = n$ has been excluded. In the sum $\lambda_1 = \sum_{i=0}^n a_{i,1}$, we can assume that $a_{0,1} \ge 1$. By these assumptions, we see that $0 < p \le b_0 < q - 1$, hence from our definition of $\mathcal{M}'_R$ we have

$$f'_k = f_k.$$

Since the exponent b_0 in f_k is not equal to 1, applying the group ring element $h \in RG$ in Lemma 6.2, we get

$$hf'_k = hf_k = -J(T^{-1}, T^{b_0}) T(x_0^{b_0-1} x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}). \tag{7.1}$$

Set $T(x_0^{b_0-1} x_1^{b_1+1} x_2^{b_2} \cdots x_n^{b_n}) := f_\ell \in \mathcal{M}_R$. The type of f_ℓ is $(s_0, s_1+1, s_2, \dots, s_{t-1})$ because we have increased λ_0 by p and decreased λ_1 by 1. Also note that $b_0 - 1$ is still strictly between 0 and $q - 1$, so $f_\ell = f'_\ell \in \mathcal{M}'_R$. As for the coefficient of f_ℓ in (7.1), Theorem 6.1 tells us that p divides $J(T^{-1}, T^{b_0})$ exactly once, because when 1 is added to $q - 1 - b_0$ there is exactly one carry: from the ones place to the p-place of the sum. Since $p^{\beta_k} | \eta_{1,r}(f'_k)$ and $\eta_{1,r}$ is an RG-module homomorphism, we have

$$p^{\beta_k} | \eta_{1,r}(hf'_k).$$

Since $p \parallel J(T^{-1}, T^{b_0})$, we get

$$p^{(\beta_k - 1)} \mid \eta_{1,r}(f'_\ell),$$

where the type of f'_ℓ is $(s_0, s_1 + 1, s_2, \ldots, s_{t-1})$. Since we assumed that α_k is the smallest such that $\alpha_k < \beta_k$, we must conclude that

$$\sum_{j=0}^{t-1} \max\{0, r - s_j\} = \sum_{j=0, j\neq 1}^{t-1} \max\{0, r - s_j\} + \max\{0, r - (s_1 + 1)\}.$$

That is, $s_1 \geq r$. As s_1 is assumed to be the smallest among $s_j, 0 \leq j \leq t-1$, we see that

$$s_j \geq r,\ 0 \leq j \leq t-1, \text{ and hence } \alpha_k = 0.$$

By Lemma 7.1, $p \nmid \eta_{1,r}(f_k)$, so $p \nmid \eta_{1,r}(f'_k)$ since $f'_k = f_k$. However we have assumed that $\beta_k > \alpha_k = 0$, that is, $p | \eta_{1,r}(f'_k)$. This is a contradiction. The theorem is proved. □

The following corollary is immediate.

Corollary 7.3. *The monomial basis $\mathcal{M}_R$ is an SNF basis of $R^{\mathcal{L}_1}$ for the map $\eta_{1,r}$, and the invariant of $\eta_{1,r}$ corresponding to a monomial of type $(s_0, \ldots, s_{t-1})$ is equal to*

$$\sum_{j=0}^{t-1} \max\{0, r - s_j\}.$$

Remark 7.4. We have seen that, for each r, the $R\mathrm{GL}(n+1, q)$ homomorphism $\eta_{1,r}$ defines a filtration $\{\overline{M}_i\}$ of $\mathbb{F}_q^{\mathcal{L}_1}$ by $\mathbb{F}_q\mathrm{GL}(n+1, q)$-modules. In the case $r = n$, it follows from Theorem 7.2 and [4, Theorems A and B] that this filtration is equal to the radical filtration, the most rapidly descending filtration with semisimple factors. Equivalently, $M_i = J^i(\mathbb{F}_q^{\mathcal{L}_1})$, where J is the Jacobson radical of the group algebra $\mathbb{F}_q\mathrm{GL}(n+1, q)$.

8. The invariant factors of the incidence between points and r-flats in $\mathrm{AG}(n, q)$

In this section, we consider the incidence between points and r-flats in the affine geometry $\mathrm{AG}(n, q)$. We will view $\mathrm{AG}(n, q)$ as obtained from $\mathrm{PG}(n, q)$ by deleting a hyperplane and all the subspaces it contains. Let H_0 be the hyperplane of $\mathrm{PG}(n, q)$ given by the equation $x_0 = 0$. Then for any integer r, $0 \leq r \leq n$, the set of r-flats of $\mathrm{AG}(n, q)$ is

$$\mathcal{F}_r = \{Y \setminus (Y \cap H_0) \mid Y \in \mathcal{L}_{r+1}\}.$$

(The empty set is not considered as an r-flat for any r.) In particular, the set of points of $\mathrm{AG}(n, q)$ is $\mathcal{F}_0$. We define the incidence map

$$\eta'_{0,r} : \mathbb{Z}^{\mathcal{F}_0} \to \mathbb{Z}^{\mathcal{F}_r} \tag{8.1}$$

by letting $\eta'_{0,r}(Z) = \sum_{Y \in \mathcal{F}_r, Z \subset Y} Y$ for every $Z \in \mathcal{F}_0$, and then extending $\eta'_{0,r}$ linearly to $\mathbb{Z}^{\mathcal{F}_0}$. Similarly, we define $\eta'_{r,0}$ to be the map from $\mathbb{Z}^{\mathcal{F}_r}$ to $\mathbb{Z}^{\mathcal{F}_0}$ sending an r-flat of $\mathrm{AG}(n, q)$ to the formal sum of all points incident with it. Let A_1 be the matrix of $\eta'_{0,r}$ with respect to the standard bases of $\mathbb{Z}^{\mathcal{F}_0}$ and $\mathbb{Z}^{\mathcal{F}_r}$. We have the following counterpart of Theorem 3.1.

Theorem 8.1. *The invariant factors of A_1 are all powers of p.*

Proof. The proof is parallel to that of Theorem 3.1. We will actually work with $A_1^\top$, which is the matrix of $\eta'_{r,0} : \mathbb{Z}^{\mathcal{F}_r} \to \mathbb{Z}^{\mathcal{F}_0}$ with respect to the standard bases of $\mathbb{Z}^{\mathcal{F}_r}$ and $\mathbb{Z}^{\mathcal{F}_0}$. We define

$$\epsilon' : \mathbb{Z}^{\mathcal{F}_0} \to \mathbb{Z}$$

to be the function sending each element in $\mathcal{F}_0$ to 1. Clearly ϵ' maps $\mathbb{Z}^{\mathcal{F}_0}$ onto $\mathbb{Z}$ and $\operatorname{Im}\eta'_{r,0}$ onto $q^r\mathbb{Z}$. Thus, $\mathbb{Z}^{\mathcal{F}_0}/(\operatorname{Ker}\epsilon' + \operatorname{Im}\eta'_{r,0}) \cong \mathbb{Z}/q^r\mathbb{Z}$, and we are reduced to proving that $(\operatorname{Ker}\epsilon' + \operatorname{Im}\eta'_{r,0})/\operatorname{Im}\eta'_{r,0}$ is a p-group. The proof goes in exactly the same way as that of Theorem 3.1. Note that $\operatorname{Ker}(\epsilon')$ is spanned by elements in $\mathbb{Z}^{\mathcal{F}_0}$ of the form $u - w$, where u and w are distinct points of $\mathrm{AG}(n,q)$; so it is enough to show that $q^r(u-w) \in \operatorname{Im}(\eta'_{r,0})$ for any two distinct points u and w. We pick an $(r+1)$-flat containing the two distinct points u and w and let $\tilde{\eta}'_{0,r}$ be the restricted map. The number of r-flats through one point in $\mathrm{AG}(r+1,q)$ is $(q^{r+1}-1)/(q-1)$ while the number of r-flats through two points in $\mathrm{AG}(r+1,q)$ is $(q^r-1)/(q-1)$, so we get

$$\eta'_{r,0}(\tilde{\eta}'_{0,r}(z)) = q^r z + \frac{q^r-1}{q-1}\mathbf{j}_U$$

for any point z. Therefore

$$\eta'_{r,0}(\tilde{\eta}'_{0,r}(u-w)) = q^r(u-w).$$

This completes the proof. □

In view of the above theorem, we view A_1 as a matrix with entries from $R = \mathbb{Z}_p[\xi_{q-1}]$. The Smith normal form of A_1 over R will completely determine the Smith normal form of A_1 over $\mathbb{Z}$. We will get the p-adic invariants of A_1 from the invariants of the incidence between points and projective r-spaces in $\mathrm{PG}(n,q)$ and those of the incidence between points and projective r-spaces in $\mathrm{PG}(n-1,q)$.

Let A be the matrix of the incidence map $\eta_{1,r+1} : R^{\mathcal{L}_1} \to R^{\mathcal{L}_{r+1}}$ with respect to the standard bases of $R^{\mathcal{L}_1}$ and $R^{\mathcal{L}_{r+1}}$. We want to partition A into a certain block form. For this purpose, we define

$$\mathcal{L}_1^{H_0} = \{Z \in \mathcal{L}_1 \mid Z \subseteq H_0\}$$

and

$$\mathcal{L}_{r+1}^{H_0} = \{Y \in \mathcal{L}_{r+1} \mid Y \subseteq H_0\}.$$

So we have the partitions

$$\mathcal{L}_1 = \mathcal{F}_0 \cup \mathcal{L}_1^{H_0}$$

and

$$\mathcal{L}_{r+1} = \mathcal{F}_r \cup \mathcal{L}_{r+1}^{H_0}.$$

We now partition A as

$$A = \left[\begin{array}{c|c} \overbrace{A_1}^{\mathcal{F}_0} & \overbrace{A_2}^{\mathcal{L}_1^{H_0}} \\ \hline 0 & A_3 \end{array}\right] \begin{array}{l} \}\mathcal{F}_r \\ \}\mathcal{L}_{r+1}^{H_0} \end{array}$$

where A_3 is the incidence matrix of the incidence between $\mathcal{L}_1^{H_0}$ and $\mathcal{L}_{r+1}^{H_0}$, which can be thought as the matrix of the incidence between points and projective r-spaces in $\mathrm{PG}(n-1,q)$.

In order to obtain the SNF of A_1, we need to modify the monomial basis $\mathcal{M}_R$ of $R^{\mathcal{L}_1}$ slightly. We replace the constant monomial in $\mathcal{M}_R$ by $T(x_0^{q-1}x_1^{q-1}\cdots x_n^{q-1})$ and denote the resulting set by $\mathcal{M}_R^*$. Note that $\mathcal{M}_R^*$ is still a basis of $R^{\mathcal{L}_1}$ because

$(1-a_0^{q-1})(1-a_1^{q-1})\cdots(1-a_n^{q-1})=0$ for each point $(a_0,a_1,\ldots,a_n)$ of $\mathrm{PG}(n,q)$. Furthermore $\mathcal{M}_R^*$ is an SNF basis of $R^{\mathcal{L}_1}$ for $\eta_{1,r+1}$ since $\mathcal{M}_R$ is an SNF basis of $R^{\mathcal{L}_1}$ for $\eta_{1,r+1}$ and the invariant corresponding to $T(x_0^{q-1}x_1^{q-1}\cdots x_n^{q-1})$ is 1. So we have the factorization

$$P^*D=AQ^*, \tag{8.2}$$

where the columns of Q^* are the basis vectors in M_R^* written with respect to the standard basis of $R^{\mathcal{L}_1}$, P^* is nonsingular over R and D is the Smith normal form of A.

We now partition $\mathcal{M}_R^*$ as $\mathcal{B}_1\cup\mathcal{B}_2$, where

$$\mathcal{B}_1=\{T(x_0^{b_0}x_1^{b_1}\cdots x_n^{b_n})\mid b_0\neq 0, T(x_0^{b_0}x_1^{b_1}\cdots x_n^{b_n})\in\mathcal{M}_R^*\}$$

and

$$\mathcal{B}_2=\{T(x_0^{b_0}x_1^{b_1}\cdots x_n^{b_n})\mid b_0=0, T(x_0^{b_0}x_1^{b_1}\cdots x_n^{b_n})\in\mathcal{M}_R^*\}.$$

We partition the matrix Q^* according to the partition of $\mathcal{M}_R^*$ as $\mathcal{B}_1\cup\mathcal{B}_2$ and the partition of $\mathcal{L}_1$ as $\mathcal{F}_0\cup\mathcal{L}_1^{H_0}$. Explicitly we have

$$Q^*=\left[\begin{array}{c|c} \overbrace{Q_1}^{\mathcal{B}_1} & \overbrace{Q_2}^{\mathcal{B}_2} \\ \hline 0 & Q_3 \end{array}\right]\begin{array}{l}\}\mathcal{F}_0\\ \}\mathcal{L}_1^{H_0}\end{array}$$

where the columns of Q_3 are the basis vectors in $\{f|_{H_0}\mid f\in\mathcal{B}_2\}$ written with respect to the standard basis of $R^{\mathcal{L}_1^{H_0}}$.

Now we rewrite (8.2) according to the block forms of the matrices A and Q^*. We have

$$\begin{pmatrix} P_1 & P_3 & P_5 \\ 0 & P_2 & P_4 \end{pmatrix}\begin{pmatrix} D_1 & 0 \\ 0 & D_2 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} A_1 & A_2 \\ 0 & A_3 \end{pmatrix}\begin{pmatrix} Q_1 & Q_2 \\ 0 & Q_3 \end{pmatrix} \tag{8.3}$$

which gives us

$$P_1D_1=A_1Q_1$$

and

$$P_2D_2=A_3Q_3.$$

Since P_1 and Q_1 inherit the property that the reductions modulo $\mathfrak{p}$ of their columns are linearly independent, D_1 must be the Smith normal form of A_1. By Corollary 7.3, $\{f|_{H_0}\mid f\in\mathcal{B}_2\}$ is an SNF basis of $R^{\mathcal{L}_1^{H_0}}$ for the incidence map $\eta_{1,r+1}$ between points and projective r-spaces in $\mathrm{PG}(n-1,q)$. We see that D_2 is the Smith normal form of A_3.

For any $n\geq 2$, $1<i\leq n$, and $\alpha\geq 0$, let $m(\alpha,n,i)$ denote the multiplicity of p^α as a p-adic invariant of the incidence between points and projective $(i-1)$-dimensional subspaces in $\mathrm{PG}(n,q)$. (The numbers $m(\alpha,n,i)$ are determined by Theorem 3.3.) We have the following theorem.

Theorem 8.2. *The p-adic invariants of A_1 are p^α, $0\leq\alpha\leq rt$, with multiplicity $m(\alpha,n,r+1)-m(\alpha,n-1,r+1)$.*

Proof. From (8.3), we see that the multiplicity of p^α as an invariant of A_1 is equal to the number of times p^α appears in D minus the number of times p^α appears in D_2. □

References

[1] M. F. Atiyah, I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Co., Reading (1969). MR0242802 (39:4129)

[2] E. F. Assmus, Jr., J. D. Key, *Designs and Their Codes*, Cambridge University Press, Cambridge (1992). MR1192126 (93j:51003)

[3] J. Ax, The zeroes of polynomials over finite fields, *Amer. J. Math.* **86** (1964), 255-261. MR0160775 (28:3986)

[4] M. Bardoe, P. Sin, The permutation modules for $\mathrm{GL}(n+1,\mathbb{F}_q)$ acting on $\mathbb{P}^n(\mathbb{F}_q)$ and $\mathbb{F}_q^{n+1}$, *J. London Math. Soc.* **61** (2000), 58-80. MR1745400 (2001f:20103)

[5] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, vol. 1, Second edition, Cambridge University Press, Cambridge, 1999.

[6] S. Black, R. J. List, On certain abelian groups associated with finite projective geometries, *Geometriae Dedicata* **33** (1990), 13-19. MR1042620 (90m:05033)

[7] D. B. Chandler, *The Smith normal forms of designs with classical parameters*, Ph.D. thesis, University of Delaware, 2004.

[8] D. B. Chandler, Q. Xiang, The invariant factors of some cyclic difference sets, *J. Combin. Theory* Ser. A **101** (2003), 131-146. MR1953284 (2004c:05034)

[9] P. M. Cohn, *Algebra*, Volume 1, John Wiley and Sons, Chichester (1974). MR0360046 (50:12496)

[10] B. Dwork, On the rationality of the zeta function of an algebraic variety, *Amer. J. Math.* **82** (1960), 631–648. MR0140494 (25:3914)

[11] A. Frumkin, A. Yakir, Rank of inclusion matrices and modular representation theory, *Israel J. Math.* **71** (1990), 309–320. MR1088823 (91m:15002)

[12] D. G. Glynn, J. W. P. Hirschfeld, On the classification of geometric codes by polynomial functions, *Designs, Codes and Cryptography* **6** (1995), 189–204. MR1351843 (97b:94031)

[13] C. D. Godsil, Problems in algebraic combinatorics, *The Electronic Journal of Combinatorics* **2** (1995), Feature 1. MR1312732 (96b:05051)

[14] N. Hamada, The rank of the incidence matrix of points and d-flats in finite geometries, *J. Sci. Hiroshima Univ.* Ser. A-I **32** (1968), 381-396. MR0243903 (39:5221)

[15] W. M. Kantor, On incidence matrices of finite projective and affine spaces, *Math. Z.* **124** (1972), 315–318. MR0377681 (51:13850)

[16] E. S. Lander, *Topics in algebraic coding theory*, D. Phil. Thesis, Oxford University, 1980.

[17] R. Liebler, personal communication (2002).

[18] P. Sin, The elementary divisors of the incidence matrices of points and linear subspaces in $P^n(\mathbb{F}_p)$, *J. Algebra* **232** (2000), 76–85. MR1783914 (2001g:20060)

[19] K. J. C. Smith, *Majority decodable codes derived from finite geometries*, Mimeograph Series 561, Institute of Statistics, Chapel Hill, NC, 1967.

[20] L. Stickelberger, Über eine Verallgemeinerung der Kreistheilung, *Math. Annalen* **37** (1890), 321–367.

[21] D. Wan, A Chevalley-Warning approach to p-adic estimates of character sums, *Proc. Amer. Math. Soc.* **123** (1995), no. 1, 45–54. MR1215208 (95c:11147)

[22] R. M. Wilson, A diagonal form for the incidence matrix of t-subsets vs. k-subsets, *European J. Combin.* **11** (1990), 609–615. MR1078717 (91i:05010)

Department of Mathematical Sciences, University of Delaware, Newark, Delaware 19716

E-mail address: chandler@math.udel.edu

Current address: Institute of Mathematics, Academia Sinica, NanGang, Taipei 11529, Taiwan

Department of Mathematics, University of Florida, Gainesville, Florida 32611

E-mail address: sin@math.ufl.edu

Department of Mathematical Sciences, University of Delaware, Newark, Delaware 19716

E-mail address: xiang@math.udel.edu