Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Journal of Algebra 318 (2007) 871–892
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

The permutation action of finite symplectic groups of odd characteristic on their standard modules ☆

David B. Chandler [a], Peter Sin [b,*], Qing Xiang [c]

[a] *Institute of Mathematics, Academia Sinica, Nangang, Taipei 11529, Taiwan*
[b] *Department of Mathematics, University of Florida, Gainesville, FL 32611, USA*
[c] *Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA*

Received 13 February 2007

Available online 14 September 2007

Communicated by Martin Liebeck

Abstract

We study the space of functions on a finite-dimensional vector space over a field of odd order as a module for a symplectic group. We construct a basis of this module with the following special properties. Each submodule generated by a single basis element under the symplectic group action is spanned as a vector space by a subset of the basis and has a unique maximal submodule. From these properties, the dimension and composition factors of the submodule generated by any subset of the basis can be determined. These results apply to incidence geometry of the symplectic polar space, yielding the symplectic analogue of Hamada's additive formula for the p-ranks of the incidence matrices between points and flats. A special case leads to a closed formula for the p-rank of the incidence matrix between the points and lines of the symplectic generalized quadrangle over a field of odd order. Together with earlier results on the 2-ranks, this result completes the determination of the p-ranks for these quadrangles.

Keywords: Generalized quadrangle; General linear group; p-Rank; Partial order; Symplectic group; Symplectic polar space

☆ Research supported in part by NSF Grant DMS 0400411.
* Corresponding author.
E-mail addresses: chandler@math.sinica.edu.tw (D.B. Chandler), sin@math.ufl.edu (P. Sin), xiang@math.udel.edu (Q. Xiang).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2007.08.020

1. Introduction

Let $k = \mathbb{F}_q$ 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 a $2m$-dimensional vector space over k. We denote by $\mathrm{PG}(2m-1, q)$ the $(2m-1)$-dimensional projective geometry of V, and denote by P the set of points of $\mathrm{PG}(2m-1, q)$. The incidence matrices between P and flats of $\mathrm{PG}(2m-1, q)$ have been studied extensively over the past forty years. See for example, [2,5–7,15] for $\mathbb{F}_p$-ranks of these matrices, and [3,13] for their Smith normal forms. The spaces $k[P]$ and $k[V]$ of k-valued functions on P and V, respectively, are permutation modules for the general linear group $\mathrm{GL}(V)$ and were investigated from this viewpoint in [2], where the p-ranks of the above incidence matrices were obtained as a corollary of the description of the submodule lattice of $k[P]$ (see [2]).

In this paper we assume that V has the additional structure of a nonsingular alternating bilinear form. Then it is natural to consider the *symplectic polar space* $\mathrm{W}(2m-1, q)$ whose flats are those flats of $\mathrm{PG}(2m-1, q)$ which are totally isotropic with respect to the form. Thus, the set of points is P and the incidence matrices between P and the flats of this geometry are submatrices of the ones above. To study these new incidence matrices we consider the spaces $k[P]$ and $k[V]$ as permutation modules for the symplectic group $\mathrm{Sp}(V)$ of the form. Let $\mathcal{I}_r$ denote the set of totally isotropic r-dimensional subspaces of V, where $1 \leqslant r \leqslant m$. The space $k[\mathcal{I}_r]$ of functions from $\mathcal{I}_r$ to k has a standard basis in bijection with $\mathcal{I}_r$ and we shall often identify the two sets. Then for $1 \leqslant r \leqslant m$ the incidence matrix between P and $\mathcal{I}_r$ is the matrix, in the standard bases, of the incidence map

$$\eta_r : k[\mathcal{I}_r] \to k[P] \tag{1}$$

sending a totally isotropic r-dimensional subspace of V to its characteristic function in $k[P]$. We are therefore interested in the images of the maps η_r.

When $q = p$ is an odd prime, the p-ranks were determined in [14] and the invariant factors of the incidence matrices over the integers were found in [9].

We now survey the results of this paper, which are valid for an arbitrary power q of an odd prime p. A crucial step is the construction of a special basis of $k[V]$ (see Definition 4.1), whose elements are called *symplectic basis functions*. Our main theorems describe the submodule structure of the $k\,\mathrm{Sp}(V)$-module generated by an arbitrary symplectic basis function. We will come back to this submodule structure later in this introduction. The $k\,\mathrm{Sp}(V)$-module $k[P]$ can be viewed as a direct summand of $k[V]$, and the images of the incidence maps η_r belong to the class of submodules of $k[V]$ generated by symplectic basis functions. From the results on submodule structure, we obtain an additive p-rank formula (Theorem 6.2) for the incidence matrix between $\mathcal{I}_1 = P$ and $\mathcal{I}_r$. This formula is the symplectic analogue of Hamada's p-rank formula [6]. In the case where $m = 2$, the additive formula leads to an attractive closed formula for the p-rank, which we will now describe in some detail.

For convenience, let $A^m_{1,r}(q)$ be a $(0,1)$-matrix with rows indexed by the elements Y of $\mathcal{I}_r$ and columns indexed by the elements Z of P, and with the (Y, Z) entry equal to 1 if and only if $Z \subseteq Y$. We consider the case where $m = 2$ (and $r = 2$) in particular. In this case, the symplectic polar space $\mathrm{W}(3, q)$ is a classical *generalized quadrangle* (GQ) [11,17], whose points are all the points of $\mathrm{PG}(3, q)$, and whose lines are the totally isotropic 2-dimensional subspaces of V. When $q = 2^t$, Sastry and Sin [12] gave the following formula for the 2-rank of $A^2_{1,2}(q)$.

$$\mathrm{rank}_2\big(A^2_{1,2}(2^t)\big) = 1 + \left(\frac{1+\sqrt{17}}{2}\right)^{2t} + \left(\frac{1-\sqrt{17}}{2}\right)^{2t}. \tag{2}$$

In the case where $q = p$ is an odd prime, de Caen and Moorhouse [4] determined the p-rank of $A^2_{1,2}(p)$, which was later generalized in [14], giving the p-ranks of $A^m_{1,r}(p)$, where $1 \leqslant r \leqslant m$, p is an odd prime, and m is not necessarily 2. In this paper, we obtain the following formula for the p-rank of $A^2_{1,2}(p^t)$, p an odd prime, as a corollary of our submodule structure results.

Theorem 1.1. *Let p be an odd prime and let $t \geqslant 1$ be an integer. Then the p-rank of $A^2_{1,2}(p^t)$ is equal to*

$$1 + \alpha_1^t + \alpha_2^t,$$

where

$$\alpha_1, \alpha_2 = \frac{p(p+1)^2}{4} \pm \frac{p(p+1)(p-1)}{12}\sqrt{17}. \tag{3}$$

We remark that in (3), if we simply set $p = 2$, then we actually obtain (2), but the two results require different proofs. We also mention in passing that the 2-rank of $A^2_{1,2}(p^t)$, where p is odd, was computed in [1].

The paper is organized as follows. In Section 2, we will review the results in [2] concerning the $\mathrm{GL}(V)$-submodule lattice of $k[V]$. The submodule lattice has a combinatorial description in terms of certain partially ordered sets $\mathcal{H}$ and $\mathcal{H}[d]$. (See Subsection 2.1 below.) For the moment, we will just consider $\mathcal{H}$, which is associated with the nontrivial summand Y_P of $k[P]$. The module Y_P has a special basis, and to each basis element there is an associated element of $\mathcal{H}$ called its $\mathcal{H}$-type, giving a surjective map from the basis to $\mathcal{H}$. It was proved in [2] that for each $\mathbf{s} \in \mathcal{H}$, the set of basis elements whose $\mathcal{H}$-types are $\leqslant \mathbf{s}$ span a $k\,\mathrm{GL}(V)$-submodule $Y(\mathbf{s})$ of Y_P with the property that $Y(\mathbf{s})$ has a unique maximal submodule. Furthermore, every submodule of Y_P is a sum of submodules of the form $Y(\mathbf{s})$.

On the representation-theoretic side, the main goal of this paper is to construct analogues of these objects adapted to the action of $\mathrm{Sp}(V)$. In order to do so, it is necessary first to look deeper into the $k\,\mathrm{GL}(V)$-structure of $k[V]$. By considering its multiplicative structure as a $k\,\mathrm{GL}(V)$-algebra, we derive tensor product factorizations of certain subquotients of $k[V]$ which will be needed in our later constructions. These new results concerning $\mathrm{GL}(V)$ are also included in Section 2. In Section 3, we define posets $\mathcal{S}$ and $\mathcal{S}[d]$ whose elements are pairs $(\mathbf{s}, \epsilon)$, with $\mathbf{s}$ in $\mathcal{H}$ (or $\mathcal{H}[d]$) and ϵ a certain "signature." In Section 4, we define a special basis of $k[V]$. Just as in the $\mathrm{GL}(V)$ case, a certain subset of this basis spans Y_P and there is a surjection from this subset to $\mathcal{S}$. For $(\mathbf{s}, \epsilon) \in \mathcal{S}$, let $Y(\mathbf{s}, \epsilon)$ be the k-subspace spanned by the basis elements of Y_P which map into the ideal in $\mathcal{S}$ determined by $(\mathbf{s}, \epsilon)$. In Section 5 we prove that $Y(\mathbf{s}, \epsilon)$ is a $k\,\mathrm{Sp}(V)$-submodule of Y_P, and our main technical result, that $Y(\mathbf{s}, \epsilon)$ has a unique maximal submodule. Unlike the $k\,\mathrm{GL}(V)$-submodules, not every $\mathrm{Sp}(V)$-submodule of Y_P is the sum of submodules of the form $Y(\mathbf{s}, \epsilon)$. The reason is a fundamental difference between the two cases. As a $k\,\mathrm{GL}(V)$-module, Y_P is multiplicity-free—that is, no two composition factors are isomorphic—while the $k\,\mathrm{Sp}(V)$-module is not. Nevertheless, the portion of the entire $k\,\mathrm{Sp}(V)$-submodule lattice generated by the submodules $Y(\mathbf{s}, \epsilon)$ is sufficiently rich for our applications. In Section 6, we apply the results of Section 5 to the images of the incidence maps η_r defined in (1) in order to obtain a summation formula for the p-rank of the incidence matrix $A^m_{1,m}(p^t)$. Theorem 1.1 is then deduced from the $m = 2$ case of this formula.

The following assumptions and notations will be in force throughout the paper. To avoid trivial exceptions, we will assume that V has dimension $2m \geqslant 4$. Let $\langle -, - \rangle$ denote the nonsingular alternating bilinear form on V. We fix a basis $e_1, e_2, \ldots, e_m, f_m, \ldots, f_1$ of V, with corresponding coordinates $x_1, x_2, \ldots, x_m, y_m, \ldots, y_1$ so that $\langle e_i, f_j\rangle = \delta_{ij}$, $\langle e_i, e_j\rangle = 0$, and $\langle f_i, f_j\rangle = 0$.

2. Action of GL(V) on $k[V]$

Throughout Sections 2 through 5 of the paper, we assume that p is an odd prime, $k = \mathbb{F}_q$, V is a $2m$-dimensional vector space over k, and $q = p^t$, $t > 1$. The assumption that $t > 1$ is mainly for notational convenience, and is only seriously used in Lemmas 5.4 and 5.5. We shall need to apply some of the results of [2].

The results in [2, Theorems A, B, C] give a simple and complete description of the $k\,\mathrm{GL}(V)$-submodule structure of the space $k[V]$ of k-valued functions on a finite vector space V. Let $k[X_1, X_2, \ldots, X_{2m}]$ denote the polynomial ring, in $2m$ variables. Since every function on V is given by a polynomial in the $2m$ coordinates x_i, the map $X_i \mapsto x_i$ defines a surjective k-algebra homomorphism $k[X_1, X_2, \ldots, X_{2m}] \to k[V]$, with kernel generated by the elements $X_i^q - X_i$. Furthermore, this map is simply the coordinate description of the following canonical map. The polynomial ring is isomorphic to the symmetric algebra $S(V^*)$ of the dual space of V; so we have a natural evaluation map $S(V^*) \to k[V]$. This canonical description makes it clear that the map is equivariant with respect to the natural actions of $\mathrm{GL}(V)$ on these spaces. A basis for $k[V]$ is obtained by taking monomials in $2m$ coordinates x_i such that the degree in each variable is at most $q-1$. We will call these the *basis monomials* of $k[V]$.

The space $k[V]$ has the structure of a $\mathbb{Z}/(q-1)\mathbb{Z}$-graded $\mathrm{GL}(V)$-algebra, where the grading is given by the characters of the center, the scalar multiplications, isomorphic to $k^\times$. Thus,

$$k[V] = \bigoplus_{[d]\in\mathbb{Z}/(q-1)\mathbb{Z}} A[d],$$

where $\mu \in k^\times$ acts on the component $A[d]$ as $\mu^{[d]}$. The component $A[d]$ has basis consisting of the basis monomials in which the total degree is in the residue class $[d]$.

2.1. Types and $\mathcal{H}$-types

We now recall the definitions of two t-tuples associated with each basis monomial. Let

$$f = \prod_{i=1}^{2m} x_i^{b_i} = \prod_{j=0}^{t-1}\prod_{i=1}^{2m} \bigl(x_i^{a_{ij}}\bigr)^{p^j}, \tag{4}$$

be a basis monomial, where $b_i = \sum_{j=0}^{t-1} a_{ij} p^j$ and $0 \leqslant a_{ij} \leqslant p-1$. Let $\lambda_j = \sum_{i=1}^{2m} a_{ij}$. The t-tuple $\boldsymbol{\lambda} = (\lambda_0, \ldots, \lambda_{t-1})$ is called the *type* of f. The set of all types of monomials is denoted by $\boldsymbol{\Lambda}$.

Let d be the integer between 0 and $q-2$ which is congruent to the total degree $\sum_i b_i = \sum_j \lambda_j p^j$ modulo $q-1$, and let $(d_0, \ldots, d_{t-1})$ be the t-tuple of p-adic digits of d.

In [2], there is another t-tuple associated with each basis monomial, which we will call its *$\mathcal{H}$-type.* If $[d] \neq [0]$ this tuple will lie in the set

$$\mathcal{H}[d] = \bigl\{\mathbf{s} = (s_0, \ldots, s_{t-1}) \bigm| \forall j,\ 0 \leqslant s_j \leqslant 2m-1,\ 0 \leqslant ps_{j+1} - s_j + d_j \leqslant 2m(p-1)\bigr\},$$

and if $d = 0$, it will belong to the set $\mathcal{H}[0] = \mathcal{H} \cup \{(0, 0, \dots, 0), (2m, 2m, \dots, 2m)\}$, where

$$\mathcal{H} = \{\mathbf{s} = (s_0, s_1, \dots, s_{t-1}) \mid \forall j,\ 1 \leqslant s_j \leqslant 2m - 1,\ 0 \leqslant ps_{j+1} - s_j \leqslant 2m(p-1)\}.$$

The $\mathcal{H}$-type $\mathbf{s}$ of f is uniquely determined by the type via the equations

$$\lambda_j = ps_{j+1} - s_j + d_j, \quad 0 \leqslant j \leqslant t - 1,$$

where the subscripts are taken modulo t. Moreover, these equations determine a bijection between the set $\boldsymbol{\Lambda}$ of types of basis monomials and the union of the sets $\mathcal{H}[d]$, $0 \leqslant d \leqslant q - 2$. We will consider the sets $\mathcal{H}[d]$ and $\mathcal{H}$ as partially ordered sets under their natural order induced by the product order on t-tuples of natural numbers.

Notation 2.1. We will be considering many objects indexed by $\mathcal{H}$-types. To indicate that the corresponding $\mathcal{H}$-type belongs to $\mathcal{H}[d]$, a decoration $[d]$ will be used. In the case $[d] = [0]$, we will most often be interested in the case where the $\mathcal{H}$-type is in $\mathcal{H}$. In this case, we adopt the convention of omitting $[0]$ from the notation.

2.2. *Composition factors*

The types, or equivalently the $\mathcal{H}$-types parametrize the composition factors of $k[V]$ in the following sense. Except for the existence of two trivial direct summands in $A[0]$, the $k\,\mathrm{GL}(V)$-module $k[V]$ is multiplicity-free. We can associate to each $\mathcal{H}$-type $\mathbf{s} \in \mathcal{H}[d]$ a composition factor, which we shall denote by $L(\mathbf{s})[d]$, such that these simple modules are all nonisomorphic except that $L((0, \dots, 0))[0] \cong L((2m, \dots, 2m))[0] \cong k$. The simple modules $L(\mathbf{s})[d]$ occur as subquotients of $k[V]$ in the following way. For $\mathbf{r} \in \mathcal{H}[d]$ let $Y(\mathbf{r})[d]$ be the span of all basis monomials with $\mathcal{H}$-types in $\mathcal{H}[d]_{\mathbf{r}} = \{\mathbf{r}' \in \mathcal{H}[d] \mid \mathbf{r}' \leqslant \mathbf{r}\}$. By [2], if $[d] \neq [0]$ then $Y(\mathbf{r})[d]$ is a $k\,\mathrm{GL}(V)$-submodule of $A[d]$ with a unique maximal submodule and such that the quotient by the maximal submodule is isomorphic to $L(\mathbf{r})[d]$. Similarly in the case $[d] = [0]$, for each $\mathbf{s} \in \mathcal{H}$, we let $Y(\mathbf{s})$ be the subspace spanned by monomials of $\mathcal{H}$-types in $\mathcal{H}_{\mathbf{s}} = \{\mathbf{s}' \in \mathcal{H} \mid \mathbf{s}' \leqslant \mathbf{s}\}$, and $Y(\mathbf{s})$ has a unique simple quotient, isomorphic to $L(\mathbf{s}) := L(\mathbf{s})[0]$ (by the notational convention above).

The isomorphism type of the simple module $L(\mathbf{s})[d]$ is most easily described in terms of the corresponding type $(\lambda_0, \dots, \lambda_{t-1}) \in \boldsymbol{\Lambda}$. Let S^{λ} be the degree λ component in the truncated polynomial ring $k[X_1, X_2, \dots, X_{2m}]/(X_i^p;\ 1 \leqslant i \leqslant 2m)$. Here λ ranges from 0 to $2m(p-1)$. Note that the dimension of S^{λ} is

$$d_{\lambda} = \sum_{j=0}^{\lfloor \lambda/p \rfloor} (-1)^j \binom{2m}{j} \binom{2m - 1 + \lambda - jp}{2m - 1}. \tag{5}$$

The simple module $L(\mathbf{s})[d]$ is isomorphic to the twisted tensor product

$$S^{\lambda_0} \otimes \left(S^{\lambda_1}\right)^{(p)} \otimes \cdots \otimes \left(S^{\lambda_{t-1}}\right)^{(p^{t-1})}. \tag{6}$$

Remark 2.2. Note that each module $(S^{\lambda})^{(p^j)}$ is itself isomorphic to a composition factor $L(\mathbf{s})[p^j\lambda]$ of $k[V]$, corresponding to the type $\boldsymbol{\lambda}$ with $\lambda_j = \lambda$ and all other components zero. Let us be more precise about this identification. From the definition, we may view $(S^{\lambda})^{(p^j)}$ as the degree λ component of the truncated polynomial ring in the variables $X_i^{p^j}$. In $k[X_1, \dots, X_{2m}]$ we consider the set of p^jth powers of monomials of total degree λ and with the degree of each variable between 0 and $p-1$. This set maps injectively into the truncated polynomial ring in the variables $X_i^{p^j}$ and the images form a basis for $(S^\lambda)^{(p^j)}$. The images of the same monomials in $k[V]$ are basis monomials of type $\boldsymbol{\lambda}$. Hence they lie in $Y(\mathbf{s})[p^j\lambda]$ and they map bijectively to a basis of the simple quotient $L(\mathbf{s})[p^j\lambda]$. Later on, when we abuse notation slightly and speak of $(S^\lambda)^{(p^j)}$ as having a basis consisting of images of basis monomials of type $\boldsymbol{\lambda}$, the exact meaning will always be as we have just described.

2.3. *Submodule structure*

The reason for considering $\mathcal{H}$-types is that they allow a simple description of the submodule structure of the $k\,\mathrm{GL}(V)$-modules $A[d]$. Suppose first that $[d]=[0]$. The space $A[0]$ has a trivial direct summand spanned by the characteristic function of $\{0\}$, which is the kernel of the natural map $A[0]\to k[P]$. The basis monomials with types in $\mathcal{H}[0]$, excluding the type $(2m(p-1), 2m(p-1), \dots, 2m(p-1))$ span a complementary direct summand, which maps isomorphically onto $k[P]$. We have

$$A[0] \cong k \oplus k[P] = k \oplus k \oplus Y_P, \tag{7}$$

where Y_P is the kernel of the map $k[P]\to k$, $f\mapsto |P|^{-1}\sum_{Q\in P} f(Q)$. The $k\,\mathrm{GL}(V)$ module Y_P is an indecomposable module whose composition factors are parametrized by $\mathcal{H}$. The [2, Theorem A] states that given any $k\,\mathrm{GL}(V)$-submodule of Y_P, the set of its composition factors is an ideal in the partially ordered set $\mathcal{H}$ and that this correspondence is an order isomorphism from the submodule lattice of Y_P to the lattice of ideals in $\mathcal{H}$. For a submodule $A \leqslant Y_P$, let $\mathcal{H}(A)\subseteq\mathcal{H}$ denote the ideal of $\mathcal{H}$-types of its composition factors.

For $[d]\neq[0]$, the set $\mathcal{H}[d]$ parametrizes the composition factors of $A[d]$ and we have a similar order isomorphism from the submodule lattice of $A[d]$ to the lattice of ideals in $\mathcal{H}[d]$, with its natural partial order [2, Theorem C]. Let $\mathcal{H}[d](A)$ denote the ideal of the submodule $A\leqslant A[d]$.

Assume now that M is a subquotient of $A[d]$ with no trivial submodules. This condition is just a convenient way of saying that in the case $[d]=[0]$ we assume M is a subquotient of Y_P (so that its set of $\mathcal{H}$-types is well defined). Then there are submodules $B\leqslant C$ of $A[d]$ with no trivial submodules such that $M=C/B$. Thus, if $[d]\neq[0]$, the composition factors of M correspond to the set $\mathcal{H}[d](C)\setminus\mathcal{H}[d](B)$, which is a difference of ideals in $\mathcal{H}[d]$, while if $[d]=[0]$ the composition factors of M correspond to $\mathcal{H}(C)\setminus\mathcal{H}(B)$, a difference of ideals in $\mathcal{H}$.

The submodules of $A[d]$ and Y_P can also be described in terms of basis monomials [2, Theorem B]. Any submodule of $A[d]$ ($[d]\neq[0]$) or of Y_P has a basis consisting of the basis monomials which it contains. Moreover, the $\mathcal{H}$-types of these basis monomials are precisely the $\mathcal{H}$-types of the composition factors of the submodule. Furthermore, in any composition series, the images of the monomials of a fixed $\mathcal{H}$-type form a basis of the composition factor of that $\mathcal{H}$-type. (These statements are not quite true of $A[0]$, because of the two trivial summands.)

2.4. $\mathrm{GL}(V)$*-algebra structure*

Multiplication in $k[V]$ is pointwise multiplication of functions and it is $\mathrm{GL}(V)$-equivariant, giving $k\,\mathrm{GL}(V)$-homomorphisms

$$A[d]\otimes A[d'] \to A[d+d'], \quad \text{for } [d],[d']\in \mathbb{Z}/(q-1)\mathbb{Z}.$$

Lemma 2.3. *Let $\boldsymbol{\lambda} = (\lambda_0, \ldots, \lambda_{t-1}) \in \boldsymbol{\Lambda}$ correspond to the $\mathcal{H}$-type $\mathbf{r} = (r_0, \ldots, r_{t-1}) \in \mathcal{H}[d]$. Let $[d^*] = [d - \lambda_{t-1} p^{t-1}]$ and let the $\mathcal{H}$-type $\mathbf{r}^* = (r_0^*, \ldots, r_{t-1}^*) \in \mathcal{H}[d^*]$ correspond to the type $\boldsymbol{\lambda}^* = (\lambda_0, \ldots, \lambda_{t-2}, 0)$. Then*

$$\mathbf{r}^* = \mathbf{r} + \mathbf{e}, \tag{8}$$

where the t-tuple $\mathbf{e}$ of integers depends only on $[d]$ and λ_{t-1}.

Proof. The lemma follows directly from the definitions of $\mathbf{r}$ and $\mathbf{r}^*$. Let d_j and d_j^* be the p-adic digits of the least nonnegative residues in $[d]$ and $[d^*]$ respectively. Then by definition,

$$\lambda_j = pr_{j+1} - r_j + d_j, \qquad \lambda_j^* = pr_{j+1}^* - r_j^* + d_j^*;$$

so for $0 \leqslant i \leqslant t-1$,

$$(q-1)r_i = \sum_{j=0}^{t-1} (\lambda_j - d_j) p^{(j-i)},$$

where the exponent $(j-i)$ is taken to be the least nonnegative residue modulo t. The lemma follows by comparing this formula with the similar one for r_i^*, remembering that $\lambda_i^* = \lambda_i$ for $0 \leqslant i \leqslant t-2$ and that $[d^*]$ is determined by $[d]$ and λ_{t-1}. □

Corollary 2.4. *Let $\mathcal{T} \subseteq \boldsymbol{\Lambda}$ be a set of types whose $(t-1)$th entries are all equal to λ_{t-1}. Let $\mathcal{T}^*$ be the set of types obtained from $\mathcal{T}$ by replacing λ_{t-1} by zero in the $(t-1)$th entry. Let $\mathcal{X}$ and $\mathcal{X}^*$ be the sets of corresponding $\mathcal{H}$-types which belong to $\mathcal{H}[d]$ and $\mathcal{H}[d^*]$ respectively, with the induced orderings. The following hold*:

(i) *The bijection $\mathcal{T} \to \mathcal{T}^*$ sending $\boldsymbol{\lambda}$ to $\boldsymbol{\lambda}^*$ induces an order isomorphism from $\mathcal{X}$ to $\mathcal{X}^*$.*
(ii) *$\mathcal{X}$ is a difference of ideals of $\mathcal{H}[d]$ if and only if $\mathcal{X}^*$ is a difference of ideals of $\mathcal{H}[d^*]$.*

Proof. Both follow from the previous lemma; for (ii) we note that a subset of a finite partially ordered set is a difference of ideals if and only if it satisfies the "intermediate value" condition that for any two elements in the subset, all elements in between them are also in the subset. □

Theorem 2.5. *Let M be a $k\mathrm{GL}(V)$-subquotient of $A[d]$ with no trivial submodules and let $\mathcal{X}$ denote the set of $\mathcal{H}$-types of its composition factors in $\mathcal{H}[d]$. Suppose that for some $j \in \mathbb{Z}/t\mathbb{Z}$, all tuples in $\mathcal{X}$ have the same r_j and also the same entries r_{j+1}. Let $\lambda_j = pr_{j+1} - r_j + d_j$. Let $\mathcal{T} \subseteq \boldsymbol{\Lambda}$ be the set of types corresponding to $\mathcal{X}$ and $\mathcal{T}^*$ be the set of types obtained from $\mathcal{T}$ by replacing λ_j by zero in the jth entry.*

Then in the $k\mathrm{GL}(V)$-submodule P of $A[d - p^j\lambda_j]$ generated by all monomials with types in $\mathcal{T}^*$, the k-subspace Q of P spanned by monomials whose types are not in $\mathcal{T}^*$ is a $k\mathrm{GL}(V)$-submodule. Let $N = P/Q$. Then

$$M \cong N \otimes \left(S^{\lambda_j}\right)^{(p^j)}. \tag{9}$$

Moreover, the types of N are obtained by replacing λ_j by 0 in the types of M.

Proof. Note that in the case $[d]=[0]$ our hypothesis implies that M is a subquotient of Y_P, so the set of $\mathcal{H}$-types of its composition factors is well defined. By Galois conjugation, we may assume $j=t-1$. By [2, Theorem A] $\mathcal{X}$ is a difference of ideals of $\mathcal{H}[d]$. Let $\mathcal{T}$ be the set of types $\boldsymbol{\lambda}=(\lambda_0,\dots,\lambda_{t-1})$ corresponding to $\mathcal{X}$. By hypothesis, the entry $\lambda_{t-1}=d_{t-1}+pr_0-r_{t-1}$ is the same for every type in $\mathcal{T}$. Then, by the previous corollary, the set $\mathcal{X}^*\subseteq\mathcal{H}[d^*]$, whose types form the set $\mathcal{T}^*$ of types obtained from $\mathcal{T}$ by replacing λ_{t-1} by 0 in the $(t-1)$th entry, is a difference of ideals in $\mathcal{H}[d^*]$, where $[d^*]=[d-\lambda_{t-1}p^{t-1}]$. Let $P\leqslant A[d^*]$ be the $k\,\mathrm{GL}(V)$-submodule generated by all monomials of types in $\mathcal{T}^*$. Then by [2] there exists a $k\,\mathrm{GL}(V)$-submodule $Q\leqslant P$ such that Q has as basis all the monomials of P whose types are not in $\mathcal{T}^*$, and $N=P/Q$ is a $k\,\mathrm{GL}(V)$-module with basis consisting of the bijective images of all monomials of type $\mathcal{T}^*$. Likewise, M has a basis consisting of images of all monomials whose types lie in $\mathcal{T}$. In exactly the same way, the p^{t-1}th powers of all monomials of degree λ_{t-1} form a basis of a $k\,\mathrm{GL}(V)$-subquotient S of $A[\lambda_{t-1}p^{t-1}]$ with $S\cong(S^{\lambda_{t-1}})^{(p^{t-1})}$ as $k\,\mathrm{GL}(V)$-modules.

It is clear that if we multiply each monomial of type $\mathcal{T}^*$ by the p^{t-1}th power of each monomial of degree λ_{t-1}, we obtain each monomial of type $\mathcal{T}$ exactly once. Therefore the multiplication map $A[d^*]\otimes A[\lambda_{t-1}p^{t-1}]\to A[d]$ induces a bijection of the subquotients

$$N\otimes S\cong M. \tag{10}$$

Since the multiplication map is a map of $k\,\mathrm{GL}(V)$-modules, the map (10) is a $k\,\mathrm{GL}(V)$-isomorphism. □

Remark 2.6. Let us interpret this tensor factorization in terms of a function $f\in A[d]$ which maps to a nonzero element $\overline{f}$ of M. Assume that f can be written as a product $f=f'f_j^{p^j}$, where the monomials of $f'\in A[d-p^j\lambda_j]$ have types in $\mathcal{T}^*$ and those of $f_j^{p^j}\in A[p^j\lambda_j]$ are of type $(0,\dots,0,\lambda_j,0,\dots,0)$. Then under the isomorphism of the theorem, $\overline{f}$ is mapped to $\overline{f'}\otimes\overline{f_j^{p^j}}$, where $\overline{f'}$ is the image of f' in the subquotient N of $A[d-p^j\lambda_j]$ and $\overline{f_j^{p^j}}$ is the image of $f_j^{p^j}$ in the simple subquotient S of $A[\lambda_j p^j]$.

2.5. *The modules $\overline{Y}(\mathbf{s})[d]_j$ and $\overline{Y}(\mathbf{s})_j$*

We will consider certain quotients of $Y(\mathbf{s})[d]$ and $Y(\mathbf{s})$. Let $\mathcal{X}\subset\mathcal{H}[d]_{\mathbf{s}}$ be the subset of tuples having jth and $(j+1)$th entries equal to s_j and s_{j+1} respectively and $\lambda_j=m(p-1)$. It is clear that $\mathcal{X}$ is the difference of the ideal $\mathcal{H}[d]_{\mathbf{s}}$ and an ideal of $\mathcal{H}[d]$, since it satisfies the "intermediate value" condition; so $\mathcal{X}$ is the set of tuples of a $k\,\mathrm{GL}(V)$-quotient $\overline{Y}(\mathbf{s})[d]_j$ of $Y(\mathbf{s})[d]$. Moreover, in the case $[d]=[0]$, we have $\mathcal{X}\subseteq\mathcal{H}$ and so $\overline{Y}(\mathbf{s})[0]_j$ is actually a quotient of $Y(\mathbf{s})$. The following is immediate from the theorem above.

Lemma 2.7. *There is a $k\,\mathrm{GL}(V)$-module B_j such that*

$$\overline{Y}(\mathbf{s})[d]_j\cong B_j\otimes\big(S^{m(p-1)}\big)^{(p^j)}.$$

3. The posets $\mathcal{S}$ and $\mathcal{S}[d]$

Definition 3.1. For $\boldsymbol{\lambda} \in \boldsymbol{\Lambda}$, let $\mathbf{s}$ be the corresponding $\mathcal{H}$-type in $\mathcal{H}[d]$. Set

$$J(\mathbf{s}) = \{ j \mid 0 \leqslant j \leqslant t-1,\ \lambda_j = m(p-1) \}.$$

For any $\mathbf{s}, \mathbf{s}' \in \mathcal{H}[d]$, let $Z(\mathbf{s}, \mathbf{s}') = \{ j \mid s'_j = s_j,\ s'_{j+1} = s_{j+1},\ \lambda_j = m(p-1)\}$. We define

$$\mathcal{S}[d] = \{ (\mathbf{s}, \epsilon) \mid \mathbf{s} \in \mathcal{H}[d],\ \epsilon \subseteq J(\mathbf{s}) \}.$$

In the case $[d] = [0]$, we also define

$$\mathcal{S} = \{ (\mathbf{s}, \epsilon) \mid \mathbf{s} \in \mathcal{H}, \epsilon \subseteq J(\mathbf{s}) \}.$$

We define $(\mathbf{s}', \epsilon') \leqslant (\mathbf{s}, \epsilon)$ if and only if $\mathbf{s}' \leqslant \mathbf{s}$ and $\epsilon \cap Z(\mathbf{s}', \mathbf{s}) = \epsilon' \cap Z(\mathbf{s}', \mathbf{s})$. It is not difficult to check that this defines a partial order on $\mathcal{S}[d]$ and $\mathcal{S}$; for transitivity one notes that if $\mathbf{s}'' \leqslant \mathbf{s}' \leqslant \mathbf{s}$, then $Z(\mathbf{s}'', \mathbf{s}) = Z(\mathbf{s}'', \mathbf{s}') \cap Z(\mathbf{s}', \mathbf{s})$.

Since each $\mathbf{s} \in \mathcal{H}$ or $\mathbf{r} \in \mathcal{H}[d]$ corresponds to a type $\lambda \in \boldsymbol{\Lambda}$, we can also talk about signed types $(\boldsymbol{\lambda}, \epsilon)$ corresponding to elements of $\mathcal{S}$ or $\mathcal{S}[d]$.

4. Action of $\mathrm{Sp}(V)$ on $k[V]$

We now equip V with a nonsingular alternating bilinear form $\langle -,- \rangle$, with the basis $e_1, e_2, \dots, e_m, f_m, \dots, f_1$ and the corresponding coordinates $x_1, x_2, \dots, x_m, y_m, \dots, y_1$ as given in Section 1. Accordingly, we view $S(V^*)$ as the polynomial ring generated by "symplectic indeterminates," $X_1, \dots, X_m, Y_m, \dots, Y_1$.

We will consider the submodule structures of $k[V]$, $A[d]$, and Y_P, under the action of $\mathrm{Sp}(V)$. First let us recall the known facts about composition factors (cf. [8,16]). We would like to know how a $\mathrm{GL}(V)$ composition factor (6) decomposes upon restriction to $\mathrm{Sp}(V)$. The modules S^{λ}, $0 \leqslant \lambda \leqslant 2m(p-1)$, all remain simple except when $\lambda = m(p-1)$, in which case we have

$$S^{m(p-1)} = S^+ \oplus S^-. \tag{11}$$

Here, S^+ and S^- are simple $k\,\mathrm{Sp}(V)$-modules, and

$$\dim(S^+) = (d_{(p-1)m} + p^m)/2, \qquad \dim(S^-) = (d_{(p-1)m} - p^m)/2. \tag{12}$$

We can describe S^+ and S^- as follows.

To avoid cumbersome notation involving $X_1, \dots, X_m, Y_m, \dots, Y_1$, we will use multi-index notation $X^{\boldsymbol{\alpha}} Y^{\boldsymbol{\beta}}$ for monomials, where $\boldsymbol{\alpha} = (a_1, \dots, a_m)$ and $\boldsymbol{\beta} = (b_1, \dots, b_m)$, $0 \leqslant a_i, b_i \leqslant p-1$. Further, for any multi-index $\boldsymbol{\beta}$, we define $|\boldsymbol{\beta}| = \sum_{i=1}^m b_i$, $\boldsymbol{\beta}! = \prod_{i=1}^m b_i!$, and $\overline{\boldsymbol{\beta}} = (p-1-b_1, \dots, p-1-b_m)$, and similarly define $|\boldsymbol{\alpha}|$ and $\boldsymbol{\alpha}!$. We will denote the images of monomials in the quotient module $S^{m(p-1)}$ using bars. Then [8] the map

$$\tau : S^{m(p-1)} \to S^{m(p-1)}, \quad \overline{X}^{\boldsymbol{\alpha}} \overline{Y}^{\boldsymbol{\beta}} \mapsto (-1)^{|\boldsymbol{\beta}|} \boldsymbol{\alpha}! \boldsymbol{\beta}! \overline{X}^{\overline{\boldsymbol{\beta}}} \overline{Y}^{\overline{\boldsymbol{\alpha}}} \tag{13}$$

is a $k\,\mathrm{Sp}(V)$-homomorphism with $\tau^2 = 1$.

The modules S^+ and S^- are the eigenspaces of τ for the eigenvalues $(-1)^m$ and $(-1)^{m+1}$ respectively. By Remark 2.2 the space $S^{m(p-1)}$ can be viewed as having a basis of images of basis monomials of $k[V]$. From this point of view, the eigenspaces S^+ and S^- have bases consisting of images of basis monomials of $k[V]$ of the form

$$x^{\boldsymbol{\alpha}} y^{\bar{\boldsymbol{\alpha}}} \tag{14}$$

and of sums and differences

$$x^{\boldsymbol{\alpha}} y^{\boldsymbol{\beta}} \pm (-1)^{|\boldsymbol{\beta}|+m} \boldsymbol{\alpha}!\boldsymbol{\beta}! x^{\bar{\boldsymbol{\beta}}} y^{\bar{\boldsymbol{\alpha}}} \tag{15}$$

of monomials, for $\boldsymbol{\alpha} \neq \bar{\boldsymbol{\beta}}$. The images of the monomials (14) together with those in (15) with a "+" sign form a basis of S^+ and the images of those in (15) with a "−" sign form a basis of S^-.

Definition 4.1. We will now define a new basis of $k[V]$, whose elements we will call *symplectic basis functions*. We will first define the symplectic basis functions of type $\boldsymbol{\lambda} = (\lambda_0, \lambda_1, \dots, \lambda_{t-1})$. Then we will take the union of these sets of functions over all $\boldsymbol{\lambda} \in \boldsymbol{\Lambda}$. The symplectic basis functions of type $\boldsymbol{\lambda}$ will be certain functions of the form

$$f = f_0 f_1^p \cdots f_{t-1}^{p^{t-1}}, \tag{16}$$

where each f_j, which we will call the jth digit of f, is either a basis monomial or binomial of $k[V]$ of degree λ_j. We will now describe the allowable forms of the jth digit; then the set of functions f, all of whose digits are allowable, will be the set of symplectic basis functions of type $\boldsymbol{\lambda}$. If $\lambda_j \neq (p-1)m$, then f_j can be any basis monomial of degree λ_j in which the degree in each variable is at most $p-1$. If $\lambda_j = (p-1)m$, then f_j can be any function of the form (14) or (15).

Clearly by restricting the types for the symplectic basis functions we can obtain bases for $A[d]$, and Y_P.

Definition 4.2. To each symplectic basis function of $k[V]$ we associate a pair $(\mathbf{s}, \epsilon) \in \mathcal{S}[d]$ for some $[d] \in \mathbb{Z}/(q-1)\mathbb{Z}$, as follows. If f is of type $\boldsymbol{\lambda}$, then $\mathbf{s}$ is the corresponding $\mathcal{H}$-type. The set $\epsilon \subseteq J(\mathbf{s})$, called the *signature,* is defined to be the set of $j \in J(\mathbf{s})$ for which the image of the jth digit f_j of f in $S^{m(p-1)}$ belongs to S^+.

From (6) and (11), it is clear that the $k\,\mathrm{Sp}(V)$-composition factors of $k[V]$ are given by their types, together with the additional choice of signs for each j with $\lambda_j = m(p-1)$. In terms of $\mathcal{H}$-types, we see that each $\mathcal{H}$-type gives a $k\,\mathrm{GL}(V)$-composition factor and then the choice of signs determines the simple $k\,\mathrm{Sp}(V)$ composition factor of this simple $k\,\mathrm{GL}(V)$-module. In this way, the elements of $\mathcal{S}$ label the $k\,\mathrm{Sp}(V)$-composition factors of Y_P, and those of $\mathcal{S}[d]$, $[d] \neq [0]$ label the $k\,\mathrm{Sp}(V)$-composition factors of $A[d]$. However it should be noted that different elements of $\mathcal{S}$ or $\mathcal{S}[d]$ can label isomorphic composition factors, due to the fact that $S^\lambda \cong S^{2m(p-1)-\lambda}$ as $k\,\mathrm{Sp}(V)$-modules. We will use $L(\mathbf{s}, \epsilon)[d]$ to denote the simple $k\,\mathrm{Sp}(V)$-submodule of $L(\mathbf{s})[d]$ where we take the $+$ summand for each $j \in \epsilon$ and the $-$ summand for each $j \in J(\mathbf{s}) \setminus \epsilon$. When $\mathbf{s} \in \mathcal{H}$, we may use the simpler notation $L(\mathbf{s}, \epsilon)$.

It follows from the definitions that the set of symplectic basis functions of $\mathcal{H}$-type $\mathbf{s} \in \mathcal{H}[d]$ and signature ϵ maps bijectively under the natural map $Y(\mathbf{s})[d] \to L(\mathbf{s})[d]$ to a basis of $L(\mathbf{s}, \epsilon)[d]$. We will also call ϵ the signature of $L(\mathbf{s}, \epsilon)[d]$.

The following statement is an immediate consequence of Lemma 2.7 and the decomposition of $S^{m(p-1)}$ just discussed.

Theorem 4.3. *As $k\,\mathrm{Sp}(V)$-modules, we have*

$$\overline{Y}(\mathbf{s})[d]_j \cong \big(B_j \otimes \big(S^+\big)^{(p^j)}\big) \oplus \big(B_j \otimes \big(S^-\big)^{(p^j)}\big).$$

5. The submodules $Y(\mathbf{s}, \epsilon)[d]$

Let $Y(\mathbf{s})[d]_j^+$ be the preimage in $Y(\mathbf{s})[d]$ of the $+$ component of $\overline{Y}(\mathbf{s})[d]_j$ in Theorem 4.3 and let $Y(\mathbf{s})[d]_j^-$ be the preimage in $Y(\mathbf{s})[d]$ of the $-$ component. For $\epsilon \subseteq J(\mathbf{s})$, let

$$Y(\mathbf{s}, \epsilon)[d] = \bigcap_{j \in \epsilon} Y(\mathbf{s})[d]_j^+ \cap \bigcap_{j \in J(\mathbf{s}) \setminus \epsilon} Y(\mathbf{s})[d]_j^-. \tag{17}$$

Thus, $Y(\mathbf{s}, \epsilon)[d]$ is a $k\,\mathrm{Sp}(V)$-submodule of $Y(\mathbf{s})[d]$.

Lemma 5.1. *Let $(\mathbf{s}, \epsilon) \in \mathcal{S}[d]$. Then $Y(\mathbf{s}, \epsilon)[d]$ has a basis consisting of all the symplectic basis functions with signed $\mathcal{H}$-types $(\mathbf{s}', \epsilon') \leqslant (\mathbf{s}, \epsilon)$.*

Proof. Suppose $(\mathbf{s}', \epsilon') \in \mathcal{S}[d]$ with $(\mathbf{s}', \epsilon') \leqslant (\mathbf{s}, \epsilon)$ and let f be a symplectic basis function of signed type $(\mathbf{s}', \epsilon')$. We will show first that $f \in Y(\mathbf{s}, \epsilon)[d]$. Write $f = f_0 f_1^p \cdots f_{t-1}^{p^{t-1}}$ as the product of its digits raised to the appropriate powers. Let $j \in J(\mathbf{s})$. We must show that $f \in Y(\mathbf{s})[d]_j^+$ if $j \in \epsilon$ and $f \in Y(\mathbf{s})[d]_j^-$ if $j \in J(\mathbf{s}) \setminus \epsilon$.

Let $j \in J(\mathbf{s})$. If $j \in \epsilon$ and f maps to zero in $\overline{Y}(\mathbf{s})[d]_j$ then f is in both $Y(\mathbf{s})[d]_j^+$ and $Y(\mathbf{s})[d]_j^-$. The similar statement holds for $j \in J(\mathbf{s}) \setminus \epsilon$. So we may assume that f has nonzero image $\overline{f} \in \overline{Y}(\mathbf{s})[d]_j$. According to Remark 2.6, under the isomorphism of Lemma 2.7, $\overline{f}$ is mapped to $\overline{f}' \otimes \overline{f}_j^{p^j}$, where $\overline{f}_j^{p^j}$ is the image of $f_j^{p^j}$ in $(S^{m(p-1)})^{(p^j)}$ and $\overline{f}'$ is the image in B_j of the product of the other factors of f. Thus, since $\overline{f} \neq 0$, we must have $j \in Z(\mathbf{s}, \mathbf{s}')$. From the definition of τ and the assumption that f_j has an allowable form, we see that $\overline{f}_j^{p^j}$ is an eigenvector of the endomorphism of $(S^{m(p-1)})^{(p^j)}$ induced by τ. Therefore $\overline{f}$ is an eigenvector of the endomorphism of $\overline{Y}(\mathbf{s})[d]_j$ induced by τ via the tensor factorization of Lemma 2.7, and will belong to either the $+$ or $-$ part of the decomposition given in Theorem 4.3. More precisely, $\overline{f}$ will be in the $+$ part if $j \in \epsilon'$ and in the $-$ part if $j \in J(\mathbf{s}') \setminus \epsilon'$. But we already have $j \in Z(\mathbf{s}, \mathbf{s}')$ and also since $(\mathbf{s}', \epsilon') \leqslant (\mathbf{s}, \epsilon)$, we have $\epsilon \cap Z(\mathbf{s}, \mathbf{s}') = \epsilon' \cap Z(\mathbf{s}, \mathbf{s}')$. Thus $\overline{f}$ is in the $+$ part if $j \in \epsilon$ and in the $-$ part if $j \notin \epsilon$. We have proved $f \in Y(\mathbf{s}, \epsilon)[d]$.

Now we must prove that $Y(\mathbf{s}, \epsilon)[d]$ is spanned by the symplectic basis functions with signed types $(\mathbf{s}', \epsilon') \leqslant (\mathbf{s}, \epsilon)$. Since we know that $Y(\mathbf{s})[d]$ has a basis consisting of all symplectic basis functions with $\mathcal{H}$-types $\mathbf{s}' \leqslant \mathbf{s}$, it suffices to prove that no linear combination

$$\sum_i c_i g_i, \tag{18}$$

with nonzero scalars c_i, of symplectic basis functions whose signed types $(\mathbf{s}_i, \epsilon_i)$ satisfy $\mathbf{s}_i \leqslant \mathbf{s}$ but $(\mathbf{s}_i, \epsilon_i) \nleqslant (\mathbf{s}, \epsilon)$, can belong to $Y(\mathbf{s}, \epsilon)[d]$. Consider the function g_1. There must exist $j \in Z(\mathbf{s}, \mathbf{s}_1)$ which belongs to ϵ but not ϵ_1, or *vice versa*. We will assume $j \in \epsilon$, as the case $j \in J(\mathbf{s}) \setminus \epsilon$ is similar. We can rewrite (18) as

$$\sum_{i \in I} c_i g_i + \sum_{r \notin I} c_r g_r,$$

where I is the set of indices i for which $j \in Z(\mathbf{s}, \mathbf{s}_i)$. Under the map $Y(\mathbf{s})[d] \to \overline{Y}(\mathbf{s})[d]_j$, the set $\{g_i \mid i \in I\}$ is mapped to a linearly independent set, while the elements g_r with $r \notin I$ are mapped to zero. The reason is that $\overline{Y}(\mathbf{s})[d]_j$ corresponds to the set of $\mathcal{H}$-types $\mathbf{s}' \leqslant \mathbf{s}$ for which $s'_j = s_j$, $s'_{j+1} = s_{j+1}$, and $\lambda'_j = m(p-1)$. Therefore, the image in $\overline{Y}(\mathbf{s})[d]_j$ of $\sum_{i \in I} c_i g_i$ is a sum of linearly independent eigenvectors for the endomorphism induced by τ. At least one of the terms, namely the image g_1, has the opposite eigenvalue to that prescribed by ϵ. The conclusion is that the image of $\sum_{i \in I} c_i g_i$ in $\overline{Y}(\mathbf{s})[d]_j$ cannot be in the $+$ component of $\overline{Y}(\mathbf{s})[d]_j$ as given in Theorem 4.3. Therefore $\sum_i c_i g_i$ cannot belong to $Y(\mathbf{s}, \epsilon)[d]$. The proof is complete. □

It is obvious from Lemma 5.1 that $Y(\mathbf{s}', \epsilon')[d] \leqslant Y(\mathbf{s}, \epsilon)[d]$ if and only if $(\mathbf{s}', \epsilon') \leqslant (\mathbf{s}, \epsilon)$. We define $Y_<(\mathbf{s}, \epsilon)[d]$ to be the kernel of the natural map $Y(\mathbf{s}, \epsilon)[d] \to L(\mathbf{s}, \epsilon)[d]$, or equivalently, the sum of all $Y(\mathbf{s}', \epsilon')[d]$ with $(\mathbf{s}', \epsilon') \lneqq (\mathbf{s}, \epsilon)$.

Remark 5.2. For $\mathbf{s} \in \mathcal{H}[d]$, we define its *digit sum* by $|\mathbf{s}| = \sum_{j=0}^{t-1} s_j$. It is not hard to see that if $(\mathbf{s}', \epsilon') \lneqq (\mathbf{s}, \epsilon)$ then there exists $(\mathbf{s}'', \epsilon'')$ such that $|\mathbf{s}''| = |\mathbf{s}| - 1$ and $(\mathbf{s}', \epsilon') \leqslant (\mathbf{s}'', \epsilon'') \leqslant (\mathbf{s}, \epsilon)$; so we also have

$$Y_<(\mathbf{s}, \epsilon)[d] = \sum_{\substack{(\mathbf{s}', \epsilon') \leqslant (\mathbf{s}, \epsilon) \\ |\mathbf{s}'| = |\mathbf{s}| - 1}} Y(\mathbf{s}', \epsilon')[d]. \tag{19}$$

5.1. Submodule structure of $Y(\mathbf{s}, \epsilon)[d]$

Lemma 5.3. *Let $\mathbf{s} \in \mathcal{H}[d]$. Then no two $k\,\mathrm{Sp}(V)$ composition factors of $\bigoplus_{\mathbf{s}'} L(\mathbf{s}')[d]$ are isomorphic, where the sum runs over all $\mathbf{s}'$ which are immediately below $\mathbf{s}$.*

Proof. Let $\mathbf{s}'$ and $\mathbf{s}'' \in \mathcal{H}[d]$ be immediately below $\mathbf{s}$. It is clear that no two simple $k\,\mathrm{Sp}(V)$-submodules of $L(\mathbf{s}')[d]$ are isomorphic; so we only need to consider the case where some $L(\mathbf{s}', \epsilon')[d]$ is isomorphic to some $L(\mathbf{s}'', \epsilon'')[d]$. Now these simple modules have the form of twisted tensor products, which, by Steinberg's Tensor Product Theorem can be isomorphic only if the corresponding tensor factors are isomorphic. Thus, the above isomorphism can only happen if $L(\mathbf{s}')[d]$ and $L(\mathbf{s}'')[d]$ are isomorphic as $k\,\mathrm{Sp}(V)$-modules, which means that for each j we must have either $\lambda'_j = \lambda''_j$ or $2m(p-1) - \lambda''_j$. Let $\mathbf{s} = (s_0, \ldots, s_{t-1})$, with similar notation for $\mathbf{s}'$ and $\mathbf{s}''$. By Galois conjugation we may assume without loss of generality that $s'_0 = s_0 - 1$ and $s''_k = s_k - 1$ for some $k \neq 0$. Suppose first $t > 2$ and $k \neq 1$. Then $\lambda'_0 = \lambda_0 + 1$ and $\lambda''_0 = \lambda_0$, so that the above condition cannot hold. If $k = 1$, then by considering $\lambda'_1 = \lambda_1$ and $\lambda''_1 = \lambda_1 + 1$, we reach the same conclusion. Finally we must consider the case $t = 2$. Then the above condition forces $2\lambda_0 = 2\lambda_1 = (2m+1)(p-1)$. Therefore $s_0 = s_1$ and so $\lambda_0 = (p-1)s_0$. Dividing the previous equation by $(p-1)$ yields the desired contradiction. □

Fix $[d] \in \mathbb{Z}/(q-1)\mathbb{Z}$ and $(\mathbf{s}, \epsilon) \in \mathcal{S}[d]$.

Let $\mathcal{Z}$ be the set of elements of $\mathcal{S}[d]$, which are immediately below $(\mathbf{s}, \epsilon)$. Let $R = \sum_{(\mathbf{s}'', \epsilon'') \in \mathcal{Z}} Y_<(\mathbf{s}'', \epsilon'')[d]$. Then

$$Y_<(\mathbf{s}, \epsilon)[d]/R \cong \bigoplus_{(\mathbf{s}'', \epsilon'') \in \mathcal{Z}} \big(Y(\mathbf{s}'', \epsilon'')[d]/Y_<(\mathbf{s}'', \epsilon'')[d]\big)$$

is a multiplicity-free semisimple module by Lemma 5.3. Fix $(\mathbf{s}', \epsilon') \in \mathcal{Z}$ and let

$$K(\mathbf{s}', \epsilon') = Y_<(\mathbf{s}', \epsilon')[d] + \sum_{\substack{(\mathbf{s}'' \epsilon'') \in \mathcal{Z} \\ (\mathbf{s}'', \epsilon'') \neq (\mathbf{s}', \epsilon')}} Y(\mathbf{s}'', \epsilon'')[d],$$

and let $U = Y(\mathbf{s}, \epsilon)[d]/Y_<(\mathbf{s}, \epsilon)[d]$. Then we have a short exact sequence

$$0 \to \big(Y(\mathbf{s}', \epsilon')[d] + K(\mathbf{s}', \epsilon')\big)/K(\mathbf{s}', \epsilon') \to Y(\mathbf{s}, \epsilon)[d]/K(\mathbf{s}', \epsilon') \to U \to 0 \tag{20}$$

which is an extension of $L(\mathbf{s}, \epsilon)[d]$ by $L(\mathbf{s}', \epsilon')[d]$.

We will show that the short exact sequence (20) does not split. To do so, we need to introduce some shift operators (elements in the group ring $k\,\mathrm{Sp}(V)$). The p-adic version of these shift operators was used extensively in [3]. Here we are using the finite field version of these operators. For $\mu \in k^\times$, we use g_μ to denote the symplectic transvection sending x_1 to $x_1 + \mu y_1$ and fixing all other coordinates.

Lemma 5.4. *For $0 \leqslant j \leqslant t-1$ and $1 \leqslant \ell \leqslant p-1$, let*

$$g_\ell(j) = \sum_{\mu \in k^\times} \mu^{\ell p^j} g_{\mu^{-1}} \in k\,\mathrm{Sp}(V). \tag{21}$$

Given any basis monomial $f = x_1^{a_1} y_1^{b_1} \cdots x_m^{a_m} y_m^{b_m}$ of $k[V]$, we have

$$g_\ell(j) f = \begin{cases} 0, & \text{if the } j\text{th digit of } a_1 \text{ is less than } \ell; \\ -\binom{a_1}{\ell p^j} x_1^{a_1 - \ell p^j} y_1^{b_1 + \ell p^j} x_2^{a_2} y_2^{b_2} \cdots x_m^{a_m} y_m^{b_m}, & \text{otherwise.} \end{cases}$$

Proof. We first prove the lemma for $j = 0$. If $a_1 = 0$, then clearly we have $g_\ell(0) f = 0$. So we assume that $a_1 > 0$.

$$\begin{aligned} g_\ell(0) f &= \sum_{\mu \in k^\times} \mu^\ell \big(x_1 + \mu^{-1} y_1\big)^{a_1} y_1^{b_1} x_2^{a_2} y_2^{b_2} \cdots x_m^{a_m} y_m^{b_m} \\ &= \left(\sum_{\mu \in k^\times} \mu^\ell \left(x_1^{a_1} + \binom{a_1}{1} \mu^{-1} x_1^{a_1 - 1} y_1 + \binom{a_1}{2} \mu^{-2} x_1^{a_1 - 2} y_1^2 + \cdots \right) \right) \\ &\quad \times y_1^{b_1} x_2^{a_2} y_2^{b_2} \cdots x_m^{a_m} y_m^{b_m} \\ &= -\binom{a_1}{\ell} x_1^{a_1 - \ell} y_1^{b_1 + \ell} x_2^{a_2} y_2^{b_2} \cdots x_m^{a_m} y_m^{b_m}. \end{aligned}$$

By a classical theorem of Lucas [10], $\binom{a_1}{\ell} \equiv 0 \pmod p$ if the 0th digit of a_1 (in the base p expansion of a_1) is less than ℓ, proving the lemma for $j = 0$.

The general case follows from the $j = 0$ case by using the Frobenius automorphism. □

We let $h_\ell(j)$ denote the group ring element analogous to $g_\ell(j)$, but with the roles of x_1 and y_1 exchanged, so that this element shifts ℓp^j from the exponent of y_1 to that of x_1.

Lemma 5.5. *For each pair of integers (α, β), $0 \leqslant \alpha, \beta \leqslant p-1$, and each j, $0 \leqslant j \leqslant t-1$, there is a group ring element $g_{\alpha,\beta}(j) \in k\,\mathrm{Sp}(V)$ such that for any basis monomial*

$$f = \prod_{i=1}^{m} x_i^{a_i} y_i^{b_i} \tag{22}$$

of $k[V]$, where $a_i = \sum_{k=0}^{t-1} a_{ik} p^k$ and $b_i = \sum_{k=0}^{t-1} b_{ik} p^k$, $0 \leqslant a_{ik}, b_{ik} \leqslant p-1$,

$$g_{\alpha,\beta}(j) f = \begin{cases} f, & \text{if } a_{1j} = \alpha \text{ and } b_{1j} = \beta, \text{ or } a_{1j} = p-1-\beta \text{ and } b_{1j} = p-1-\alpha; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. It suffices to prove the lemma in the case where $\alpha + \beta \leqslant p-1$. The reason is that for any pair (α, β), $0 \leqslant \alpha, \beta \leqslant p-1$, with $\alpha + \beta > p-1$, the "complementary" pair $(p-1-\beta, p-1-\alpha)$ has sum of entries equal to $2(p-1) - (\alpha + \beta)$, which is $< p-1$, and $g_{p-1-\beta, p-1-\alpha}(j)$ will be the required element. We will only give the proof for the $j = 0$ case. The other cases are the same. We use induction on $\alpha + \beta$.

First assume that $\alpha + \beta = p-1$. Using Lemma 5.4, we define

$$g_{\alpha,\beta}(0) = -\binom{p-1}{\beta}^{-1} g_\beta(0) h_{p-1}(0) g_\alpha(0). \tag{23}$$

We claim that $g_{\alpha,\beta}(0)$ has the required action on the basis monomials of $k[V]$. It can be seen as follows. Let f be a basis monomial of $k[V]$ as in (22). We first assume that $a_{10} + b_{10} \leqslant p-1$. By Lemma 5.4,

$$g_\alpha(0) f = \begin{cases} -\binom{a_{10}}{\alpha} x_1^{a_1-\alpha} y_1^{b_1+\alpha} x_2^{a_2} y_2^{b_2} \cdots x_m^{a_m} y_m^{b_m}, & \text{if } a_{10} \geqslant \alpha; \\ 0, & \text{otherwise.} \end{cases}$$

Next,

$$h_{p-1}(0)\bigl(g_\alpha(0) f\bigr) = \begin{cases} \binom{a_{10}}{\alpha} x_1^{a_1-\alpha+p-1} y_1^{\sum_{k=1}^{t-1} b_{1k} p^k} x_2^{a_2} y_2^{b_2} \cdots x_m^{a_m} y_m^{b_m}, \\ \qquad \text{if } a_{10} \geqslant \alpha \text{ and } b_{10} + \alpha = p-1; \\ 0, \quad \text{otherwise.} \end{cases}$$

Note that since $\alpha + \beta = p-1$, we have $b_{10} + \alpha = p-1$ if and only if $b_{10} = \beta$. So

$$h_{p-1}(0)\bigl(g_\alpha(0) f\bigr) = \begin{cases} \binom{a_{10}}{\alpha} x_1^{a_1-b_{10}} y_1^{\sum_{k=1}^{t-1} b_{1k} p^k} x_2^{a_2} y_2^{b_2} \cdots x_m^{a_m} y_m^{b_m}, & \text{if } a_{10} \geqslant \alpha \text{ and } b_{10} = \beta; \\ 0, & \text{otherwise.} \end{cases}$$

Finally,

$$g_\beta(0)\big(h_{p-1}(0)g_\alpha(0)f\big)=\begin{cases}-\binom{p-1}{\beta}\binom{a_{10}}{\alpha}x_1^{a_1}y_1^{b_1}x_2^{a_2}y_2^{b_2}\cdots x_m^{a_m}y_m^{b_m}, & \text{if } a_{10}\geqslant\alpha \text{ and } b_{10}=\beta;\\ 0, & \text{otherwise.}\end{cases}$$

Note that under the assumptions $\alpha+\beta=p-1$ and $a_{10}+b_{10}\leqslant p-1$, the condition that $a_{10}\geqslant\alpha$ and $b_{10}=\beta$ means exactly $a_{10}=\alpha$ and $b_{10}=\beta$. We have shown that the group ring element defined in (23) has the desired action on those f with $a_{10}+b_{10}\leqslant p-1$.

For the purpose of this lemma, two monomials f and f' can be considered "complementary," if $f=\prod_{i=1}^m x_i^{a_i}y_i^{b_i}$ and $f'=\prod_{i=1}^m x_i^{a_i'}y_i^{b_i'}$ with $a_{10}+b_{10}'=a_{10}'+b_{10}=p-1$. The elements we are constructing should act the same on f' and on f. In particular, the element (23) acts the same on f' as it does on f. That is,

$$g_{\alpha,\beta}(j)f'=\begin{cases}f', & \text{if } a_{10}=\alpha \text{ and } b_{10}=\beta;\\ 0, & \text{otherwise.}\end{cases}$$

The analysis is quite similar to the above. (One needs to take extra care when there is a carry from the 0th digit to the first digit, such as in the case where $p-1-a_{10}+\alpha\geqslant p$. We omit the details.) With this observation, we see that the group ring element defined in (23) also has the desired action on those f with $a_{10}+b_{10}>p-1$, proving the base case where $\alpha+\beta=p-1$.

For a general pair (α,β) with $\alpha+\beta<p-1$, by induction hypothesis, we may assume that for all those pairs (γ,δ), $0\leqslant\gamma,\delta\leqslant p-1$, with $\alpha+\beta<\gamma+\delta<p$, we have found $g_{\gamma,\delta}(0)$ with the desired property. We define

$$g_{\alpha,\beta}(0)=-\binom{\alpha+\beta}{\beta}^{-1}g_\beta(0)h_{(\alpha+\beta)}(0)g_\alpha(0)\prod_{\alpha+\beta<\gamma+\delta<p}\big(1-g_{\gamma,\delta}(0)\big).$$

Again we claim that this $g_{\alpha,\beta}(0)$ has the required action on the basis monomials as given in the statement of the lemma. Clearly, if $\alpha+\beta<a_{10}+b_{10}<2(p-1)-(\alpha+\beta)$, then f will be annihilated by $\prod_{\alpha+\beta<\gamma+\delta<p}(1-g_{\gamma,\delta}(0))$. So we only need to consider the action of $g_{\alpha,\beta}(0)$ on those f with

$$a_{10}+b_{10}\leqslant\alpha+\beta<p-1\quad\text{or}\quad p-1<2(p-1)-(\alpha+\beta)\leqslant a_{10}+b_{10}.$$

It is clear that $\prod_{\alpha+\beta<\gamma+\delta<p}(1-g_{\gamma,\delta}(0))$ acts on such basis monomials as the identity, and we only need to consider the action of $-\binom{\alpha+\beta}{\beta}^{-1}g_\beta(0)h_{(\alpha+\beta)}(0)g_\alpha(0)$ on these monomials.

Now if $a_{10}+b_{10}<p$, an analysis similar to that in the $\alpha+\beta=p-1$ case shows that

$$-\binom{\alpha+\beta}{\beta}^{-1}g_\beta(0)h_{(\alpha+\beta)}(0)g_\alpha(0)(f)=\begin{cases}f, & \text{if } a_{10}=\alpha \text{ and } b_{10}=\beta;\\ 0, & \text{otherwise,}\end{cases}$$

and in the complementary case $a_{10}+b_{10}\geqslant p-1$,

$$-\binom{\alpha+\beta}{\beta}^{-1}g_\beta(0)h_{(\alpha+\beta)}(0)g_\alpha(0)(f')=\begin{cases}f', & \text{if } a_{10}'+\beta=p-1 \text{ and } \alpha+b_{10}'=p-1;\\ 0, & \text{otherwise.}\end{cases}$$

The proof is complete. □

Lemma 5.6. *Assume that* $(\mathbf{s}, \epsilon)$ *is not a minimal element of* $\mathcal{S}[d]$. *If* $[d] = [0]$ *we assume in addition that* $(\mathbf{s}, \epsilon) \in \mathcal{S}$ *and is not minimal in* $\mathcal{S}$. *Then the short exact sequence* (20) *does not split.*

Proof. We will choose a particular element $f \in Y(\mathbf{s}, \epsilon)[d]$ with nonzero image in

$$U = Y(\mathbf{s}, \epsilon)[d]/Y_{<}(\mathbf{s}, \epsilon)[d]$$

and show that if $f^* \in Y(\mathbf{s}, \epsilon)[d]$ is any element with the same image in U, then as a $k\,\mathrm{Sp}(V)$-module, $Y(\mathbf{s}, \epsilon)[d]/K(\mathbf{s}', \epsilon')$ is generated by the image of f^* in $Y(\mathbf{s}, \epsilon)[d]/K(\mathbf{s}', \epsilon')$. Let us first fix some notation. Since $\mathbf{s}'$ is immediately below $\mathbf{s}$, there is a unique index $j+1$ where these two tuples differ and $s'_{j+1} = s_{j+1} - 1$. We let $\boldsymbol{\lambda}$ and $\boldsymbol{\lambda}'$ be the types corresponding to $\mathbf{s}$ and $\mathbf{s}'$, respectively.

The element f is chosen to be a certain symplectic basis function of signed $\mathcal{H}$-type $(\mathbf{s}, \epsilon)$. Since $(s_0, \ldots, s_j, s_{j+1} - 1, s_{j+2}, \ldots, s_{t-1}) \in \mathcal{H}[d]$, we have $\lambda_j \geqslant p$ and $\lambda_{j+1} < 2m(p-1)$. Therefore we may choose f such that the jth digit of the exponent of x_1 is at least 1 and the jth digit of the exponent of y_1 is equal to $p-1$. We can also require that the $(j+1)$th digit of the exponent of y_1 be less than $p-1$, and further, if $\lambda_{j+1} = m(p-1)-1$, that the $(j+1)$th digits of the exponents of x_1 and y_1 be 0. Let f_j denote the jth digit of f.

Let $e = f^* - f \in Y(\mathbf{s}', \epsilon')[d] + K(\mathbf{s}', \epsilon')$. From the definition of symplectic basis functions f^* has the form

$$f^* = f_0 f_1^p \cdots \left(x_1^a y_1^{p-1} \cdots\right)^{p^j} f_{j+1}^{p^{j+1}} \cdots f_{t-1}^{p^{t-1}} + e$$

or

$$f^* = f_0 f_1^p \cdots \left(x_1^a y_1^{p-1} \cdots \pm c x_1^0 y_1^{p-1-a} \cdots\right)^{p^j} f_{j+1}^{p^{j+1}} \cdots f_{t-1}^{p^{t-1}} + e,$$

where $a \geqslant 1$, c represents the product of factorials as in (15), and f_{j+1} could be a monomial or another term of the same form as in (14) or (15).

Now we apply the group ring element $g_{a,p-1}(j)$ from Lemma 5.5 to f^*. It annihilates all but those monomials appearing in e with the same jth digits of the exponents of x_1 and y_1 as those of f or the complementary jth digits, 0 and $p-1-a$, respectively. Next we apply the shift operator $g_1(j)$ from Lemma 5.4 which shifts p^j from the exponent of x_1 to that of y_1. The results are

$$\begin{aligned} &g_1\left(f_0 f_1^p \cdots \left(x_1^a y_1^{p-1} \cdots\right)^{p^j} f_{j+1}^{p^{j+1}} \cdots f_{t-1}^{p^{t-1}}\right) \\ &\quad = f_0 f_1^p \cdots \left(x_1^{a-1} y_1^0 \cdots\right)^{p^j} (f_{j+1} y_1)^{p^{j+1}} \cdots f_{t-1}^{p^{t-1}}, \end{aligned} \tag{24}$$

which is of $\mathcal{H}$-type $\mathbf{s}'$, and

$$g_1\left(f_0 f_1^p \cdots \left(x_1^0 y_1^{p-1-a} \cdots\right)^{p^j} f_{j+1}^{p^{j+1}} \cdots f_{t-1}^{p^{t-1}}\right) = 0. \tag{25}$$

Note that if f' is any other symplectic basis function appearing in f^* belonging to $Y(\mathbf{s}', \epsilon')[d] + K(\mathbf{s}', \epsilon')$, not annihilated by $g_{a,p-1}(j)$, then $g_1(f') \in K(\mathbf{s}', \epsilon')$ because the $\mathcal{H}$-type of $g_1(f')$ is obtained by subtracting 1 from the $(j+1)$th entry of the $\mathcal{H}$-type of f'. Now we have produced an element (24) of $(Y(\mathbf{s}',\epsilon')[d]+K(\mathbf{s}',\epsilon'))$ and we must show that it is not zero, modulo $K(\mathbf{s}',\epsilon')$, or in other words, that when this element is expressed in symplectic basis functions, necessarily of $\mathcal{H}$-type $\mathbf{s}'$, some symplectic basis function of signature ϵ' appears with nonzero coefficient. Since $(\mathbf{s}',\epsilon')\leqslant(\mathbf{s},\epsilon)$ and the tuples $\mathbf{s}$ and $\mathbf{s}'$ differ only in the $(j+1)$st digit, we have $Z(\mathbf{s},\mathbf{s}')\subseteq J(\mathbf{s}')\subseteq Z(\mathbf{s},\mathbf{s}')\cup\{j,j+1\}$. We consider several possibilities. If $J(\mathbf{s}')=Z(\mathbf{s},\mathbf{s}')$ then all basis functions involved in (24) are of signature ϵ'. If $j\in J(\mathbf{s}')$, that is to say $\lambda'_j=m(p-1)$, then in (24) the jth digit of the exponent of x_1 is at most $p-2$, and that of y_1 is 0. The monomial is not of the form (14) and therefore can be written as the sum of a (nonzero) S^+ term and a (nonzero) S^- term. Similarly, if $\lambda'_{j+1}=m(p-1)$, we have taken care that the $(j+1)$th digits of the exponents of x_1 and y_1 are 0 and 1, and the monomial is not of the form (14). Thus, for all four possibilities for $J(\mathbf{s}')$ and for any $\epsilon'\subseteq J(\mathbf{s}')$ such that $\epsilon'\cap Z(\mathbf{s},\mathbf{s}')=\epsilon\cap Z(\mathbf{s},\mathbf{s}')$, the element in (24) involves a symplectic basis function with signature ϵ'. The proof is now complete. □

Remark 5.7. If $[d]=[0]$, the assumption of Lemma 5.6 is equivalent to $\mathbf{s}\neq(0,\dots,0)$, $(2m,\dots,2m)$ or $(1,\dots,1)$.

We recall that the *radical* of a module is the intersection of its maximal submodules. Let $\operatorname{rad} M$ denote the radical of a $k\operatorname{Sp}(V)$-module M. It is the smallest submodule of M whose corresponding quotient is semisimple.

Theorem 5.8.

(i) *If* $[d]\neq[0]$ *then* $Y_<(\mathbf{s},\epsilon)[d]$ *is the unique maximal* $k\operatorname{Sp}(V)$*-submodule of* $Y(\mathbf{s},\epsilon)[d]$.
(ii) *For* $(\mathbf{s},\epsilon)\in\mathcal{S}$, $Y_<(\mathbf{s},\epsilon)$ *is the unique maximal* $k\operatorname{Sp}(V)$*-submodule of* $Y(\mathbf{s},\epsilon)$.

Proof. We may assume in both parts that $(\mathbf{s},\epsilon)$ satisfies the hypotheses of Lemma 5.6, for otherwise $Y(\mathbf{s},\epsilon)[d]$ in (i) and $Y(\mathbf{s},\epsilon)$ in (ii) are simple modules and there is nothing to prove. We will only give the argument for (ii), since the proof of (i) is formally identical. The assertion of the theorem can be restated as $\operatorname{rad} Y(\mathbf{s},\epsilon)=Y_<(\mathbf{s},\epsilon)$. We proceed by induction on the partial order of $\mathcal{S}$, the result being clear for the minimal element. Let $f\in Y(\mathbf{s},\epsilon)\setminus Y_<(\mathbf{s},\epsilon)$ and let Y_f be the $k\operatorname{Sp}(V)$ submodule generated by f. By Lemma 5.6 the sequence (20) does not split. Therefore Y_f contains an element of $Y(\mathbf{s}',\epsilon')+K(\mathbf{s}',\epsilon')$ which has nonzero image in

$$\big(Y(\mathbf{s}',\epsilon')+K(\mathbf{s}',\epsilon')\big)/K(\mathbf{s}',\epsilon')\cong Y(\mathbf{s}',\epsilon')/Y_<(\mathbf{s}',\epsilon').$$

Thus, $(Y_f+R)/R$ has $L(\mathbf{s}',\epsilon')$ as a composition factor. Since $(\mathbf{s}',\epsilon')$ was an arbitrary element of $\mathcal{Z}$ and since $Y_<(\mathbf{s},\epsilon)/R$ is multiplicity-free by Lemma 5.3, it then follows that $(Y_f+R)/R=Y(\mathbf{s},\epsilon)/R$. By the inductive hypothesis, we have $R=\sum_{(\mathbf{s}',\epsilon')\in\mathcal{Z}}\operatorname{rad} Y(\mathbf{s}',\epsilon')\leqslant\operatorname{rad} Y_<(\mathbf{s},\epsilon)$ and since $Y_<(\mathbf{s},\epsilon)/R$ is semisimple, we have $R=\operatorname{rad} Y_<(\mathbf{s},\epsilon)$. We have therefore proved that Y_f maps onto $Y(\mathbf{s},\epsilon)/\operatorname{rad} Y_<(\mathbf{s},\epsilon)$. Then Y_f contains a submodule of $Y_<(\mathbf{s},\epsilon)$ which maps onto $Y_<(\mathbf{s},\epsilon)/\operatorname{rad} Y_<(\mathbf{s},\epsilon)$. Since the radical of a module is the intersection of the maximal submodules, the above submodule of $Y_<(\mathbf{s},\epsilon)$ must be all of $Y_<(\mathbf{s},\epsilon)$. Hence Y_f contains $Y_<(\mathbf{s},\epsilon)$ and we conclude that $Y_f=Y(\mathbf{s},\epsilon)$. The theorem is proved. □

The following corollary is immediate.

Corollary 5.9. *Let* $(\mathbf{s},\epsilon)\in\mathcal{S}[d]$. *Then any* $f\in Y(\mathbf{s},\epsilon)[d]\setminus Y_<(\mathbf{s},\epsilon)[d]$ *generates* $Y(\mathbf{s},\epsilon)[d]$.

The $k\,\mathrm{GL}(V)$-radical series of $Y(\mathbf{s})[d]$ ($[d] \neq [0]$) and $Y(\mathbf{s})$ are given by digit sums as follows. Let $\mathrm{rad}^i_{\mathrm{GL}(V)} M$ denote the ith $k\,\mathrm{GL}(V)$-radical of the $k\,\mathrm{GL}(V)$-module M. Then

$$\mathrm{rad}^i_{\mathrm{GL}(V)} Y(\mathbf{s})[d] = \sum_{|\mathbf{s}'|=|\mathbf{s}|-i} Y(\mathbf{s}')[d], \tag{26}$$

with a similar equation for $Y(\mathbf{s})$. These results can be read off from [2].

Our next result gives the analogous statements for $Y(\mathbf{s},\epsilon)[d]$ and $Y(\mathbf{s},\epsilon)$.

Corollary 5.10.

(i) *If* $[d] \neq [0]$ *then*

$$\mathrm{rad}^i Y(\mathbf{s},\epsilon)[d] = \sum_{(\mathbf{s}'',\epsilon'')} Y(\mathbf{s}'',\epsilon'')[d]$$

where the sum is over all $(\mathbf{s}'',\epsilon'') \in \mathcal{S}[d]$ *such that* $(\mathbf{s}'',\epsilon'') \leqslant (\mathbf{s},\epsilon)$ *and* $|\mathbf{s}''| = |\mathbf{s}| - i$.

(ii) *If* $(\mathbf{s},\epsilon) \in \mathcal{S}$, *then*

$$\mathrm{rad}^i Y(\mathbf{s},\epsilon) = \sum_{(\mathbf{s}'',\epsilon'')} Y(\mathbf{s}'',\epsilon'')$$

where the sum is over all $(\mathbf{s}'',\epsilon'') \leqslant (\mathbf{s},\epsilon)$ *such that* $|\mathbf{s}''| = |\mathbf{s}| - i$.

Proof. We will only prove (i), since (ii) is similar. Let M_i denote the module on the right side of the equation in (i). By Remark 5.2, and Theorem 5.8 we see that M_{i+1} is the sum of all of the radicals of the $Y(\mathbf{s}',\epsilon')[d]$ occurring in M_i, and therefore $M_{i+1} \leqslant \mathrm{rad}\, M_i$, since the radical of a sum of submodules of a module contains the sum of their radicals. It remains to show that M_i/M_{i+1} is semisimple, which will show $M_{i+1} \geqslant \mathrm{rad}\, M_i$, completing the proof.

We claim that

$$M_i = \mathrm{rad}^i_{\mathrm{GL}(V)} Y(\mathbf{s})[d] \cap Y(\mathbf{s},\epsilon)[d]. \tag{27}$$

From the claim, M_i/M_{i+1} is isomorphic to a $k\,\mathrm{Sp}(V)$-submodule of the semisimple $k\,\mathrm{GL}(V)$-module $(\mathrm{rad}^i_{\mathrm{GL}(V)} Y(\mathbf{s})[d])/(\mathrm{rad}^{i+1}_{\mathrm{GL}(V)} Y(\mathbf{s})[d])$; so it is a semisimple $k\,\mathrm{Sp}(V)$-module, since every simple $k\,\mathrm{GL}(V)$-composition factor is semisimple as a $k\,\mathrm{Sp}(V)$-module. To prove our claim, we consider the basis of $Y(\mathbf{s})[d]$ consisting of all symplectic basis functions with $\mathcal{H}$-types $\leqslant \mathbf{s}$. The subset of this basis consisting of those functions whose $\mathcal{H}$-types satisfy $|\mathbf{s}'| \leqslant |\mathbf{s}| - i$ form a basis of $\mathrm{rad}^i_{\mathrm{GL}(V)} Y(\mathbf{s})[d]$, by the description of $k\,\mathrm{GL}(V)$-radical series above. By Lemma 5.1, the subset of this basis consisting of those elements whose signed types are $\leqslant (\mathbf{s},\epsilon)$ form a basis $Y(\mathbf{s},\epsilon)[d]$. And, by Lemma 5.1 and the definition of M_i, the subset of the above basis of $Y(\mathbf{s})[d]$ of functions whose signed $\mathcal{H}$-types satisfy both conditions $(\mathbf{s}',\epsilon) \leqslant (\mathbf{s}',\epsilon)$ and $|\mathbf{s}'| \leqslant |\mathbf{s}| - i$ form a basis of M_i. The claim is established and the proof complete. □

Remark 5.11. The above corollary may be restated as saying the $k\,\mathrm{Sp}(V)$-radical series of $Y(\mathbf{s},\epsilon)[d]$ and $Y(\mathbf{s},\epsilon)$ are given by intersecting the modules with the $k\,\mathrm{GL}(V)$-radical series of $Y(\mathbf{s})[d]$ and $Y(\mathbf{s})$, respectively.

6. The dimensions of $\mathrm{Im}(\eta_r)$

Recall from Section 1 that for $1 \leqslant r \leqslant m$, η_r denotes the incidence map from $k[\mathcal{I}_r]$ to $k[P]$ sending a totally isotropic r-dimensional subspace of V to its characteristic function in P. For $m+1 \leqslant r \leqslant 2m-1$, we can define $\mathcal{I}_r$ to be the set of r-dimensional subspaces of the form $W^\perp = \{v \in V \mid \langle v, w\rangle = 0$, for all $w \in W\}$, for some totally isotropic $(2m-r)$-dimensional subspace W. We can also consider the incidence maps η_r in this case.

Theorem 6.1.

(i) *We have*

$$\mathrm{Im}(\eta_m) = k1 \oplus Y(\mathbf{s}_m, \epsilon_m),$$

where $\mathbf{s}_m = (m, m, \ldots, m)$ *and* $\epsilon_m = \{0, 1, \ldots, t-1\}$.

(ii) *If* $1 \leqslant r \leqslant 2m-1$ *and* $r \neq m$, *then*

$$\mathrm{Im}(\eta_r) = k1 \oplus Y(\mathbf{s}_r),$$

where $\mathbf{s}_r = (2m-r, 2m-r, \ldots, 2m-r)$. *In particular, if* $1 \leqslant r < m$, *then the* $\mathbb{F}_q$*-code generated by the characteristic functions of all totally isotropic* r*-dimensional subspaces of* V *is equal to the* $\mathbb{F}_q$*-code generated by the characteristic functions of all* r*-dimensional subspaces of* V.

Proof. We shall assume that $t > 1$. When $t = 1$, a similar and easier argument works, but we omit the details to keep the argument clear, since this case is already known [14].

(i) Since each point of P is contained in $\prod_{i=1}^{m-1}(1+q^i)$ totally isotropic m-dimensional subspaces of V, by adding up the characteristic functions of all totally isotropic m-dimensional subspaces of V, we get a nonzero constant function. Hence $k1 \subset \mathrm{Im}(\eta_m)$, where $k1$ is the space of constant functions. Therefore we have a $k\,\mathrm{Sp}(V)$-decomposition

$$\mathrm{Im}(\eta_m) = k1 \oplus M,$$

where $M \subset Y_P$ (cf. (7)).

Let L be the totally isotropic m-dimensional subspace of V defined by the equations $x_i = 0$, $i = 1, 2, \ldots, m$, and χ_L be the characteristic function of L. Since $\mathrm{Sp}(V)$ is transitive on $\mathcal{I}_m$, we have

$$\mathrm{Im}(\eta_m) = k\,\mathrm{Sp}(V)\chi_L.$$

Note that

$$\begin{aligned}\chi_L &= \left(1 - x_1^{q-1}\right)\left(1 - x_2^{q-1}\right)\cdots\left(1 - x_m^{q-1}\right)\\ &= 1 + f,\end{aligned}$$

where $f = \sum_{\emptyset \neq I \subseteq \{1,2,\ldots,m\}} (-1)^{|I|}\mathbf{x}_I^{q-1}$, and $\mathbf{x}_I$ stands for $\prod_{i\in I} x_i$. Therefore, we have $M = k\,\mathrm{Sp}(V) f$. For $0 < |I| < m$, the monomial $\mathbf{x}_I^{q-1}$ is a symplectic basis function of signed type

$((|I|, |I|, \dots, |I|), \emptyset)$, which lies below the signed type $(\mathbf{s}_m, \epsilon_m)$ of the symplectic basis function $x_1^{q-1} x_2^{q-1} \cdots x_m^{q-1}$ in the poset $\mathcal{S}$. Hence $f \in Y(\mathbf{s}_m, \epsilon_m) \setminus Y_<(\mathbf{s}_m, \epsilon_m)$. Therefore by Corollary 5.9, we have

$$M = Y(\mathbf{s}_m, \epsilon_m).$$

We have proved (i).

(ii) First we deal with the case where $1 \leqslant r < m$. Choose L to be the totally isotropic r-dimensional subspace of V defined by the equations $x_1 = x_2 = \cdots = x_m = 0$ and $y_1 = y_2 = \cdots = y_{m-r} = 0$. Then the characteristic function of L in P is

$$\chi_L = \left(1 - x_1^{q-1}\right)\left(1 - x_2^{q-1}\right) \cdots \left(1 - x_m^{q-1}\right)\left(1 - y_1^{q-1}\right) \cdots \left(1 - y_{m-r}^{q-1}\right).$$

Since $\mathrm{Sp}(V)$ is transitive on $\mathcal{I}_r$, we have $\mathrm{Im}(\eta_r) = k\,\mathrm{Sp}(V)\chi_L$. This module also has the splitting

$$k\,\mathrm{Sp}(V)\chi_L = k1 \oplus N,$$

where $N = k\,\mathrm{Sp}(V) f$, $f = \chi_L - 1$. Note that

$$f = (-1)^r x_1^{q-1} \cdots x_m^{q-1} y_1^{q-1} \cdots y_{m-r}^{q-1} + (-1)^{r-1} x_2^{q-1} \cdots x_m^{q-1} y_1^{q-1} \cdots y_{m-r}^{q-1} + \cdots.$$

The symplectic basis function $x_1^{q-1} \cdots x_m^{q-1} y_1^{q-1} \cdots y_{m-r}^{q-1}$ has signed type $(\mathbf{s}_r, \emptyset)$. The remaining terms in f have signed types strictly less than $(\mathbf{s}_r, \emptyset)$. Hence by Corollary 5.9, we have $N = Y(\mathbf{s}_r, \emptyset)$, which in turn is equal to $Y(\mathbf{s}_r)$ since $(\mathbf{s}', \epsilon') \leqslant (\mathbf{s}_r, \emptyset)$ simply means $\mathbf{s}' \leqslant \mathbf{s}_r$. The proof of (ii) is complete in the case where $1 \leqslant r < m$. A similar argument works for the $m < r \leqslant 2m-1$ case. □

Next we give the symplectic analogue of Hamada's formula for the p-rank of the incidence matrix between points and m-flats of $\mathrm{W}(2m-1, q)$ in terms of t, where $q = p^t$, p an odd prime. In particular, we will give a proof for Theorem 1.1.

Theorem 6.2. *Let $A_{1,m}^m(p^t)$ be the incidence matrix between points and m-flats of* $\mathrm{W}(2m-1, p^t)$*, as defined in Section* 1. *Assume that p is odd. Then*

$$\mathrm{rank}_p\left(A_{1,m}^m\left(p^t\right)\right) = 1 + \sum_{\substack{(s_0,\dots,s_{t-1}) \\ (\forall j) 1 \leqslant s_j \leqslant m}} \prod_{j=0}^{t-1} d_{(s_j, s_{j+1})},$$

where

$$d_{(s_j, s_{j+1})} = \begin{cases} \dim(S^+) = (d_{m(p-1)} + p^m)/2, & \text{if } s_j = s_{j+1} = m, \\ d_{\lambda_j}, \quad \text{where } \lambda_j = p s_{j+1} - s_j, & \text{otherwise}. \end{cases}$$

Proof. By (i) of Theorem 6.1, the p-rank of $A_{1,m}^m(p^t)$ is 1 plus the dimension of $Y(\mathbf{s}_m, \epsilon_m)$, where $\mathbf{s}_m = (m, m, \dots, m)$ and $\epsilon_m = \{0, 1, \dots, t-1\}$. By Theorem 5.8, the $k\,\mathrm{Sp}(V)$ module $Y(\mathbf{s}_m, \epsilon_m)$ is multiplicity-free, and has as composition factors all $L(\mathbf{s}', \epsilon')$, $(\mathbf{s}', \epsilon') \leqslant (\mathbf{s}_m, \epsilon_m)$.

Adding up the dimensions of these composition factors (recall (5) and (12)), we obtain the summation formula for $\mathrm{rank}_p(A^m_{1,m}(p^t))$. $\square$

Corollary 6.3. *The p-rank of $A^m_{1,m}(p^t)$, when p is an odd prime, is given by*

$$\mathrm{rank}_p\big(A^m_{1,m}\big(p^t\big)\big) = 1 + \mathrm{Trace}\big(D^t\big) = 1 + \alpha_1^t + \cdots + \alpha_m^t,$$

where

$$D = \begin{pmatrix} d_{(1,1)} & d_{(1,2)} & \cdots & d_{(1,m)} \\ d_{(2,1)} & d_{(2,2)} & \cdots & d_{(2,m)} \\ \vdots & \vdots & \ddots & \vdots \\ d_{(m,1)} & d_{(m,2)} & \cdots & d_{(m,m)} \end{pmatrix},$$

and $\alpha_1, \alpha_2, \ldots, \alpha_m$ are the eigenvalues of D.

Note that some of the entries of D may be zero. We are now ready to give the proof of Theorem 1.1.

Proof of Theorem 1.1. We are dealing with W(3, p^t), i.e., the case where $m = 2$. To simplify notation, we write $A^2_{1,2}(p^t)$ simply as $A^{(t)}$. In this case, we have

$$d_{(1,1)} = \dim\big(S^{p-1}\big) = \frac{p(p+1)(p+2)}{6},$$
$$d_{(1,2)} = \dim\big(S^{2p-1}\big) = \frac{2p(p-1)(p+1)}{3},$$
$$d_{(2,1)} = \dim\big(S^{p-2}\big) = \frac{p(p+1)(p-1)}{6},$$
$$d_{(2,2)} = \dim\big(S^{+}\big) = \frac{p(p+1)(2p+1)}{6}.$$

Therefore

$$D = \frac{p(p+1)}{6}\begin{pmatrix} p+2 & 4(p-1) \\ p-1 & 2p+1 \end{pmatrix}.$$

This matrix D has two distinct eigenvalues

$$\alpha_1, \alpha_2 = \frac{p(p+1)^2}{4} \pm \frac{p(p+1)(p-1)}{12}\sqrt{17}.$$

Therefore we have

$$\mathrm{rank}_p\big(A^{(t)}\big) = 1 + \alpha_1^t + \alpha_2^t. \qquad \square$$

The case where $m = 3$ can be similarly analyzed. The matrix D in this case is given as follows.

$$D = \frac{1}{120}\begin{pmatrix} (p+4)!/(p-1)! & (p^3-p)(p+2)(26p+48) & 66p^5-210p^3+144p \\ (p+3)!/(p-2)! & 26p^5+50p^4+10p^3+10p^2+24p & 66p^5-30p^3-36p \\ (p+2)!/(p-3)! & 26p^5-10p^3-16p & 33p^5+75p^3+12p \end{pmatrix}.$$

The eigenvalues of D have very complicated expressions: we will not write down them here.

Acknowledgments

Machine computations for the case $q = 9$ and the case $q = 27$ done by Eric Moorhouse and Dave Saunders respectively were helpful in the early stages of our investigations.

References

[1] B. Bagchi, A.E. Brouwer, H.A. Wilbrink, Notes on binary codes related to the $O(5,q)$ generalized quadrangle for odd q, Geom. Dedicata 39 (1991) 339–355.

[2] 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.

[3] D.B. Chandler, P. Sin, Q. Xiang, The invariant factors of the incidence matrices of points and subspaces in $\mathrm{PG}(n,q)$ and $\mathrm{AG}(n,q)$, Trans. Amer. Math. Soc. 358 (2006) 3537–3559.

[4] D. de Caen, E. Moorhouse, The p-rank of the $\mathrm{Sp}(4,p)$ generalized quadrangle, unpublished, 1998.

[5] D.G. Glynn, J.W.P. Hirschfeld, On the classification of geometric codes by polynomial functions, Des. Codes Cryptogr. 6 (1995) 189–204.

[6] 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.

[7] S.P. Inamdar, N.S. Narasimha Sastry, Codes from Veronese and Segre embeddings and Hamada's formula, J. Combin. Theory Ser. A 96 (2001) 20–30.

[8] J. Lahtonen, On the submodules and composition factors of certain induced modules for groups of type C_n, J. Algebra 140 (1991) 415–425.

[9] J.M. Lataille, The elementary divisors of incidence matrices between certain subspaces of a finite symplectic space, J. Algebra 268 (2003) 444–462.

[10] M.E. Lucas, Sur les congruences des nombres eulériens, et des coefficients différentiels des fonctions trigonométriques, suivant un module premier, Bull. Soc. Math. France 6 (1878) 49–54.

[11] S.E. Payne, J.A. Thas, Finite Generalized Quadrangles, Res. Notes Math., vol. 110, Pitman (Advanced Publishing Program), Boston, MA, 1984.

[12] N.S.N. Sastry, P. Sin, The code of a regular generalized quadrangle of even order, in: Proc. Sympos. Pure Math., vol. 63, 1998, pp. 485–496.

[13] P. Sin, The elementary divisors of the incidence matrices of points and linear subspaces in $\mathbf{P}^n(\mathbf{F}_p)$, J. Algebra 232 (2000) 76–85.

[14] P. Sin, The permutation representation of $\mathrm{Sp}(2m,\mathbb{F}_p)$ acting on the vectors of its standard module, J. Algebra 241 (2001) 578–591.

[15] K.J.C. Smith, Majority Decodable Codes Derived from Finite Geometries, Mimeograph Ser., vol. 561, Institute of Statistics, Chapel Hill, NC, 1967.

[16] I.D. Suprunenko, A.E. Zalesskii, Reduced symmetric powers of natural realizations of the groups $\mathrm{SL}_m(P)$ and $\mathrm{Sp}_m(P)$ and their restrictions to subgroups, Siberian Math. J. 31 (4) (1990) 33–46.

[17] J. Tits, Sur la trialité et certains groupes qui s'en déduisent, Publ. Math. Inst. Hautes Études Sci. 2 (1959) 14–60.