On codes that are invariant under the affine group

Peter Sin*

Department of Mathematics
University of Florida
358, Little Hall, PO Box 118105
Gainesville, FL 32611–8105, U.S.A

sin@ufl.edu

Submitted: May 7, 2012; Accepted: Oct 9, 2012; Published: Nov 8, 2012
Mathematics Subject Classifications: 20B25, 05E18, 05E10

Abstract

Let $k[V]$ be the space of functions from a finite vector space into the algebraically closure of its field of scalars. This paper describes the lattice of subspaces of $k[V]$ which are invariant under the affine group $\mathrm{AGL}(V)$. The description provides a simple method for finding the submodule generated by any set of functions given as polynomials in the standard coordinates.

1 Introduction

This paper concerns the vector space $k[V]$ of functions from a finite vector space to an algebraically closed field of the same characteristic and its $k\mathrm{AGL}(V)$-submodules, the subspaces which are invariant under the natural action of the affine group $\mathrm{AGL}(V)$. Previously, this problem has been investigated as a topic in coding theory. The subspaces in question are precisely the codes of length $|V|$ which are $\mathrm{AGL}(V)$-invariant. In the case $n = 1$, all such codes were determined in [10]. Later, in [3], [5] the results of [10] were reformulated, giving a combinatorial description of the lattice of $\mathrm{AGL}(V)$-invariant subcodes of $k[V]$. The general case was treated in the important paper [6], yielding a characterization of the $\mathrm{AGL}(V)$-invariant subcodes of $k[V]$. The purpose of this paper is to give an explicit description of the $k\mathrm{AGL}(V)$-submodules of $k[V]$ (Theorem 9), using the standard coordinates on V, as well as a combinatorial description of the lattice of submodules (Theorem 7). In [1], a similar study was carried out for the $k\mathrm{GL}(V)$-submodules of $k[V]$ and some results from that work will be used here.

*Supported by NSF grant DMS0071060.

Much of the motivation for this work has been provided by two related topics outside coding theory.

First, there is quite a large body of research in representation theory, dating back to the origins of the subject, with the basic theme of studying invariant subspaces of polynomial rings under the action of classical groups and algebras. As a small sample we mention [8], [11], [12] and [13]; more can be found in the references of these papers. The present paper follows in this tradition, particularly from a technical standpoint. For example, the facts about simple modules in Section 3 below are standard in this theory.

A second connection is to doubly transitive permutation groups. The paper [15] raised the problem of describing the submodule structure of the doubly transitive permutation modules over all fields. The present paper supplies the answer for the permutation module in the natural characteristic for $\mathrm{AGL}(V)$ acting on V.

2 Notation and background

Let $q = p^t$ be a prime power and let $V = \mathbb{F}_q^n$ be the n-dimensional affine space over $\mathbb{F}_q$. Our principal object of study is the space $k[V]$ of functions from V to an algebraically closed field k of characteristic p. The group $\mathrm{GL}(V)$ of linear automorphisms of V and the group $\mathrm{AGL}(V) = V \rtimes \mathrm{GL}(V)$ of invertible affine transformations act on the basis V of $k[V]$, so the latter is a permutation module for these groups. If we choose coordinates for V, then $k[V]$ may be viewed as the quotient $k[x_1, \ldots, x_n]/(x_i^q - x_i)_{i=1}^n$ of the polynomial ring, with the groups $\mathrm{GL}(V)$ and $\mathrm{AGL}(V)$ acting through homogeneous and inhomogeneous linear substitutions respectively.

2.1 Twisted degrees and types of monomials

The images in $k[V]$ of the monomials $\prod_{i=1}^n x_i^{a_i}$ with $0 \leqslant a_i \leqslant q-1$ form a basis of $k[V]$. We will refer to these elements of $k[V]$ as *basic monomials*. It is clear what is meant by the degree of a basic monomial, namely the number $a_1 + \ldots + a_n$. Now the Galois group of $\mathbb{F}_q$, a cyclic group of order t, acts on $k[V]$ and in fact permutes the set of basic monomials; a generator σ raises each basic monomial to its p-th power, with the understanding that x_i^q is replaced by x_i. Given a basic monomial $m = \prod_{i=1}^n x_i^{a_i}$, we express each a_i p-adically as $a_i = \sum_{j=0}^{t-1} b_{ij} p^j$ and rewrite m as $\prod_{j=0}^{t-1} [\prod_{i=1}^n x_i^{b_{ij}}]^{p^j}$. Let $\lambda_j = \sum_{i=1}^n b_{ij}$. Then the degree of m is $\sum_j \lambda_j p^j$, and the degree of its image under σ^{-e} is $\sum_j \lambda_j p^{(j-e)}$, where the exponent $(j-e)$ is the representative of the mod t congruence class of $j-e$ in the range from 0 to $t-1$.

Based on these observations we will now asociate with each basic monomial two t-tuples of non-negative integers which will be called its *type* and its *twisted degree tuple*. These data will play a fundamental role throughout the rest of this paper.

Definition 1. Given a basic monomial

$$m = \prod_{j=0}^{t-1} [\prod_{i=1}^{n} x_i^{b_{ij}}]^{p^j} \tag{1}$$

with $0 \leqslant b_{ij} \leqslant p-1$, let $\lambda_j = \sum_{i=1}^{n} b_{ij}$. We define the *type* of m to be the t-tuple $(\lambda_0, \ldots, \lambda_{t-1})$.

The *e-th twisted degree* of m is defined to be the degree of $\sigma^{-e}(m)$, namely $\sum_j \lambda_j p^{(j-e)}$ and the *twisted degree tuple* of m to be the t-tuple $(d_0, \ldots, d_{t-1})$, where d_e is the e-th twisted degree.

For example, consider the basic monomial $x_i^{p^j}$. Its type is the j-th standard basis vector $\mathbf{e}_j$ $(0 \leqslant j \leqslant t-1)$ of $\mathbf{Z}^t$ and its twisted degree tuple is

$$\mathbf{v}_j = (p^j, \ldots, p, 1, \ldots, p^{(j+1)}). \tag{2}$$

The t-tuples $\mathbf{e}_j$ and $\mathbf{v}_j$ are related by the formula

$$p\mathbf{v}_{j-1} - \mathbf{v}_j = (q-1)\mathbf{e}_j, \quad (j = 0, \ldots, t-1). \tag{3}$$

As another example, if we set

$$\mathbf{1} = (1, 1, \ldots, 1) \tag{4}$$

then the basic monomial $\prod_{i=1}^{n} x_i^{q-1}$ has type $n(p-1)\mathbf{1}$ and twisted degree tuple $n(q-1)\mathbf{1}$.

The galois action induced on these tuples is easy to describe; the type and twisted degree tuple of $\sigma(m)$ are obtained from those for m by shifting the entries cyclically one place to the right.

It is clear that the twisted degree tuple of a basic monomial depends only on its type. Let $\mathcal{T}$ be the set of all types of basic monomials and $\mathcal{D}$ the set of all their twisted degree tuples. Then

$$\mathcal{T} = \{\boldsymbol{\lambda} = (\lambda_0, \ldots, \lambda_t) \in \mathbb{N}^t \mid \quad 0 \leqslant \lambda_i \leqslant n(p-1)\}. \tag{5}$$

Let $\Phi : \mathcal{T} \to \mathcal{D}$ be the map assigning to a type $\boldsymbol{\lambda}$ its tuple of twisted degrees. It is additive in the sense that if a type is the sum of two types, then its twisted degree tuple is the sum of the those of its summands.

Since every type can be written as a nonnegative integral combination of the $\mathbf{e}_j$, with coefficients between 0 and $n(p-1)$, we have

$$\mathcal{D} = \{\sum_{j=0}^{t-1} c_j \mathbf{v}_j \mid 0 \leqslant c_j \leqslant n(p-1)\} \tag{6}$$

The formula (3) shows that the map Φ is injective and that its image $\mathcal{D}$ lies in the sublattice

$$M = \{(z_0, \ldots, z_{t-1}) \in \mathbb{Z}^t \mid pz_j - z_{j+1} \in (q-1)\mathbb{Z}^t, j = 0, \ldots, t-1\} \tag{7}$$

of $\mathbb{Z}^t$. Moreover, it follows from (3) that M is equal to the sublattice of $\mathbb{Z}^t$ generated by $\mathcal{D}$.

Definition 2. We give $\mathcal{D}$ the structure of a poset by taking the partial order $\leqslant$ to be the one induced by the standard partial order on $\mathbb{Z}^t$, i.e. $\mathbf{z} \leqslant \mathbf{z}'$ if and only if $z_j \leqslant z'_j$ for $j = 0, \ldots, t-1$.

3 Filtrations, and composition factors

3.1 Multiplicity-free modules

We recall that a module having a Jordan-Hölder series is called *multiplicity-free* if no two composition factors are isomorphic.

Lemma 3. *(a) $k[V]$ has a unique maximal $k\mathrm{AGL}(V)$ submodule J and $k[V]/J \cong k$ is a trivial module. J has as basis the set of all basic monomials of type $\neq n(p-1)\mathbf{1}$.*

(b) The space of constant functions on V is the unique minimal submodule of $k[V]$.

(c) J is multiplicity-free as a $k\mathrm{AGL}(V)$-module (or as a $k\mathrm{GL}(V)$-module).

Proof. $\mathrm{AGL}(V)$ acts transitively on the basis V of $k[V]$ and the stablizer of the origin is $\mathrm{GL}(V)$. If S is a simple $k\mathrm{AGL}(V)$-module, then it is also simple for $\mathrm{GL}(V)$ (since the normal p-subgroup V must act trivially) and by Frobenius reciprocity, we have

$$\mathrm{Hom}_{k\mathrm{AGL}(V)}(k[V], S) \cong \mathrm{Hom}_{k\mathrm{GL}(V)}(k, S). \tag{8}$$

The first part of (a) is immediate from this. The unique basic monomial of type $n(p-1)\mathbf{1}$ is $\prod_{i=1}^{n} x_i^{q-1}$. Since all of the other basic monomials have lower degree, it follows that the subspace they span is a $k\mathrm{AGL}(V)$-submodule and that the quotient is a one-dimensional trivial module. Therefore, by the uniqueness just proved, this maximal submodule is J. The fact that $k[V]$ has a unique minimal submodule follows from (a) by the self-duality of the permutation module $k[V]$; and it is clear that the constant functions form a one-dimensional submodule, so (b) holds. Part (c) is a very well known and follows from the fact that $\mathrm{GL}(V)$ has a cyclic subgroup of order $q^n - 1$ which acts regularly (simply transitively) on $V \setminus \{0\}$. (In coding theory terms, this expresses the cyclicity of the $\mathrm{GL}(V)$-invariant subcodes of $k[V \setminus \{0\}]$.) □

Because of Lemma 3, the submodule lattice of $k[V]$ will be known once we know that of J. Further, since J is multiplicity-free, we know by general representation theory that its submodule lattice is isomorphic to the lattice of ideals in the poset in which the elements are the isomorphism classes of composition factors, partially ordered by the rule that one composition factor lies above another if and only if every submodule having the first composition factor also has the second.

3.2 The simple modules $S(\boldsymbol{\lambda})$

Next we shall define a set of simple $k\mathrm{GL}(V)$-modules parametrized by the set $\mathcal{T}$ of types of basic monomials. These will turn out to be the composition factors of $k[V]$. For $\boldsymbol{\lambda} = (\lambda_0, \dots \lambda_{t-1}) \in \mathcal{T}$, the corresponding simple module, denoted $S(\boldsymbol{\lambda})$, can be constructed in the following way. Let $V_k = k \otimes_{\mathbb{F}_q} V$. Then the algebraic group $\mathrm{GL}(V_k)$ acts (by homogeneous linear substitutions) on $k[x_1, \dots, x_n]$ and hence also on $k[x_1, \dots, x_n]/(x_i^p)_{i=1}^n$. For $0 \leqslant \lambda \leqslant n(p-1)$, let $\overline{S}^\lambda = \overline{S}^\lambda(V_k)$ denote the degree λ component of the graded algebra $k[x_1, \dots, x_n]/(x_i^p)_{i=1}^n$. Then we may form the twisted tensor product

$$S(\boldsymbol{\lambda}) = \overline{S}^{\lambda_0} \otimes (\overline{S}^{\lambda_1})^{(p)} \otimes \cdots \otimes (\overline{S}^{\lambda_{t-1}})^{(p^{t-1})}, \tag{9}$$

where the powers of p in the superscripts indicate Frobenius twists [9, I.9.10].

It is well known that the $\mathrm{GL}(V_k)$-modules obtained in this way are simple and remain simple when restricted to the finite group $\mathrm{GL}(V)$. Details and references can be found in [1, §2.3]. The dimensions and characters of the modules $S(\boldsymbol{\lambda})$ are also well known ([1, §2.4]).

3.3 Twisted Filtrations and the modules $Y_{\mathbf{d}}$

We now consider some natural filtrations of $k[V]$ which will allow us to show that the composition factors of J are the modules $S(\boldsymbol{\lambda})$ for $\boldsymbol{\lambda} \in \mathcal{T} \setminus \{n(p-1)\mathbf{1}\}$

For each natural number r the basic monomials of degree $\leqslant r$ span an $\mathrm{AGL}(V)$ submodule F_r of $k[V]$. Thus we have the *degree filtration* $0 \leqslant F_0 \leqslant F_1 \leqslant \cdots F_{n(q-1)} = k[V]$. If we let σ also denote the Frobenius map on $\mathrm{AGL}(V)$, then for $g \in \mathrm{AGL}(V)$ we have

$$g\sigma^{-e}(m) = \sigma^{-e}(\sigma^e(g)m), \tag{10}$$

which shows that the e-th twisted degree of each basic monomial occuring in gm is no greater than the e-th twisted degree of the basic monomial m. Thus we obtain a total of t filtrations by twisted degrees of $\mathrm{AGL}(V)$-modules $0 \leqslant F_0^{(j)} \leqslant F_1^{(j)} \leqslant \cdots F_{n(q-1)}^{(j)} = k[V]$, where $F_r^{(j)} = \sigma^{-j} F_r$.

For each $\mathbf{d} = (d_0, \dots, d_{t-1}) \in \mathcal{D}$ define the submodule

$$Y_{\mathbf{d}} = F_{d_0} \cap F_{d_1}^{(1)} \cap \ldots \cap F_{d_{t-1}}^{(t-1)}. \tag{11}$$

Let $Y_{<\mathbf{d}}$ be the subspace of $Y_{\mathbf{d}}$ spanned by all basic monomials with twisted degree tuples $< \mathbf{d}$. This is a $k\mathrm{AGL}(V)$-submodule.

Lemma 4. *Let $\boldsymbol{\lambda} = \Phi^{-1}(\mathbf{d})$. Then $Y_{\mathbf{d}}/Y_{<\mathbf{d}} \cong S(\boldsymbol{\lambda})$.*

Proof. It is clear from the definitons that $Y_{\mathbf{d}}/Y_{<\mathbf{d}}$ has as basis the images of all basic monomials of type $\boldsymbol{\lambda}$. The action of $\mathrm{GL}(V)$ on this module is by homogeneous linear substitution of the monomials, followed by deletion of all monomials of type different from $\boldsymbol{\lambda}$.

Consider the k-vector space isomorphism from the tensor product (9) to $Y_{\mathbf{d}}/Y_{<\mathbf{d}}$ given by

$$\otimes_{j=0}^{t-1}(\prod_i x_i^{b_{ij}})^{(p^j)} \mapsto \prod_i x_i^{\sum_j b_{ij}p^j}. \tag{12}$$

(Here we have kept the same notation for the images of basic monomials in $Y_{\mathbf{d}}/Y_{<\mathbf{d}}$.)

The action of $\mathrm{GL}(V)$ on each tensor factor in (9) is by homogeneous linear substitution of the variables followed by deletion of terms involving a p-th power or higher in any variable. Since we have an explicit description of the $\mathrm{GL}(V)$-action on both spaces, it is now elementary to verify that (12) defines a $k\mathrm{GL}(V)$-isomorphism. In checking this, two things to keep in mind are the definitions of scalar multiplication in the twisted tensor factors and the fact that in characteristic p, the p-th power of a sum is the sum of the p-th powers. □

It is immediate from Lemma 4 that each $S(\boldsymbol{\lambda})$ with $\boldsymbol{\lambda} \in T$ is a composition factor of $k[V]$. They are in fact all of the composition factors since $S(\boldsymbol{\lambda})$ has as basis (the images of) all basic monomials of type $\boldsymbol{\lambda}$, while $k[V]$ is spanned by monomials of all types. More generally, the same argument proves the following corollary.

Corollary 5. *For $\mathbf{d} \in \mathcal{D}$ composition factors of $Y_{\mathbf{d}}$ are the simple modules $S(\boldsymbol{\lambda}')$ such that $\Phi(\boldsymbol{\lambda}') \leqslant \mathbf{d}$.*

Since $J = Y_{<n(p-1)\mathbf{1}}$, its composition factors are the $S(\boldsymbol{\lambda})$ for $\boldsymbol{\lambda} \neq n(p-1)\mathbf{1}$. Lemma 3, (c) therefore implies that these simple modules are mutually non-isomorphic, while parts (a) and (b) of the same lemma show that $S(n(p-1)\mathbf{1}) \cong k \cong S(0\mathbf{1})$.

3.4 The poset $(\mathcal{T}, \preceq)$

Since the set of composition factors of J is in bijection with $\mathcal{T} \setminus \{n(p-1)\mathbf{1}\}$, the partial ordering on the composition factors of J induces a partial order on this set.

Definition 6. The partial order $\preceq$ on $\mathcal{T}$ is the extension of the above partial order on $\mathcal{T} \setminus \{n(p-1)\mathbf{1}\}$, in which $n(p-1)\mathbf{1}$ is declared to be the unique maximal element.

By virtue of Lemma 3, the lattice of ideals in $(\mathcal{T}, \preceq)$ is isomorphic to the lattice of $k\mathrm{AGL}(V)$-submodules of $k[V]$, ordered by inclusion.

The bijection $\Phi : \mathcal{T} \to \mathcal{D}$ allows us to compare the ordered sets $(\mathcal{T}, \preceq)$ and $(\mathcal{D}, \leqslant)$. Since the space $Y_{\Phi(\boldsymbol{\lambda})}$ is a $k\mathrm{AGL}(V)$-submodule of $k[V]$ having as composition factors all $S(\boldsymbol{\lambda}')$ with $\Phi(\boldsymbol{\lambda}') \leqslant \Phi(\boldsymbol{\lambda})$, it follows that Φ is order-preserving.

4 The $k\mathrm{AGL}(V)$-submodule lattice of $k[V]$

We are now ready to state our main theorems.

Theorem 7. *The map Φ is an isomorphism of partially ordered sets.*

Remark 8. Theorem 7 should be viewed as a reformulation of the characterization of affine-invariant codes in [6]. The results of [6] are not used in its proof.

Theorem 9. *(a) The submodule of $k[V]$ generated by a basic monomial m of type $\boldsymbol{\lambda}$ is equal to $Y_{\Phi(\boldsymbol{\lambda})}$.*

(b) The submodule $Y_{<\Phi(\boldsymbol{\lambda})}$ is the unique maximal submodule of $Y_{\Phi(\boldsymbol{\lambda})}$ and $Y_{\Phi(\boldsymbol{\lambda})}/Y_{<\Phi(\boldsymbol{\lambda})} \cong S(\boldsymbol{\lambda})$. The composition factors of $Y_{\Phi(\boldsymbol{\lambda})}$, each occurring with multiplicity one, are the simple modules $S(\boldsymbol{\lambda}')$, for all $\boldsymbol{\lambda}'$ such that $\Phi(\boldsymbol{\lambda}') \leqslant \Phi(\boldsymbol{\lambda})$.

(c) For $\boldsymbol{\lambda} \neq n(p-1)\mathbf{1}$ any submodule which has $S(\boldsymbol{\lambda})$ as a composition factor contains $Y_{\Phi(\boldsymbol{\lambda})}$.

(d) The submodule of $k[V]$ generated by an element $\sum \alpha_m m$, expressed as a linear combination of basic monomials, is the sum of the submodules $Y_{\Phi(\boldsymbol{\lambda})}$ as $\boldsymbol{\lambda}$ runs over the types of the basic monomials with non-zero coefficients.

Remark 10. The case $t = 1$ of Theorem 9 which is a fundamental result in the theory of generalized Reed-Muller codes, was worked out in detail in [6].

The theorems will be proved in 4.2 below, with the aid of the lemmas in the next subsection.

4.1

Lemma 11. *Let $\mathbf{d}$, $\mathbf{d}' \in \mathcal{D}$ with $\mathbf{d}' \leqslant \mathbf{d}$ and $\mathbf{d} - \mathbf{d}' \in (q-1)\mathbb{Z}^t$. Then $\Phi^{-1}(\mathbf{d}') \preceq \Phi^{-1}(\mathbf{d})$ in $\mathcal{T}$.*

Proof. In view of Lemma 3, (a) and (b), we can assume $\mathbf{d}$, $\mathbf{d}' \neq (0, \dots 0)$, $(n(q-1), \dots, n(q-1))$. The hypothesis on $\mathbf{d} - \mathbf{d}'$ implies that $S(\Phi^{-1}(\mathbf{d}))$ and $S(\Phi^{-1}(\mathbf{d}'))$ are composition factors in the same direct summand of the $k\mathrm{GL}(V)$-module $k[V]$. The submodule structure of these summands is given in [1, Theorems A and C]. (We note that there are slight notational differences; for example the tuples $\mathcal{H}$ in [1, Theorems A] should be multiplied by $q-1$ to give the corresponding twisted degree tuples.) It follows from these results that any $k\mathrm{GL}(V)$-submodule of $k[V]$ having $S(\Phi^{-1}(\mathbf{d}))$ as a composition factor also has $S(\Phi^{-1}(\mathbf{d}'))$. Hence, the same holds for $k\mathrm{AGL}(V)$-submodules. See also [6]. □

Lemma 12. *Let $\boldsymbol{\lambda} = (\lambda_0, \lambda_1, \dots, \lambda_{t-1})$ and $\boldsymbol{\lambda}' = (\lambda'_0, \lambda'_1, \dots, \lambda'_{t-1})$. Suppose that for some j, we have $\lambda'_j = \lambda_j + 1$ and $\lambda'_k = \lambda_k$ for $k \neq j$. Then $\boldsymbol{\lambda} \preceq \boldsymbol{\lambda}'$.*

Proof. By Lemma 3, we can assume $\boldsymbol{\lambda}$, $\boldsymbol{\lambda}' \neq (0,\dots,0)$, $n(p-1)\mathbf{1}$. We may also assume without loss of generality that $j = 0$. Let $\Phi(\boldsymbol{\lambda}) = \mathbf{d}$ and $\Phi(\boldsymbol{\lambda}') = \mathbf{d}'$. Set $E = Y_{\mathbf{d}'}/(\sum_{\mathbf{d}''} Y_{\mathbf{d}''})$, where the sum is over all $\mathbf{d}'' \leqslant \mathbf{d}'$ except for $\mathbf{d}'$ and $\mathbf{d}$. Now there is no element of $\mathcal{D}$ betweeen $\mathbf{d}$ and $\mathbf{d}'$, so E has a simple submodule $U \cong S(\boldsymbol{\lambda})$ with quotient $E/U \cong S(\boldsymbol{\lambda}')$. To prove the lemma, we must show that U is the unique simple submodule of E. If $q = 2$ we are in the case of the classical Reed-Muller codes. This is much simpler than the general case and it is well known and straightforward to show that $k[V]$ is uniserial, from which the lemma follows easily. We will not repeat this case here and assume from now on that $q > 2$. (An independent proof of the uniseriality of $k[V]$ in the more general case $q = p$ is given in Theorem 16 below.) Now the k-span of basic monomial m is invariant under the subgroup of scalar matrices $\mathbb{F}_q^\times I$ and the character afforded is $\alpha I \mapsto \alpha^{deg(m)}$. Since the degrees of $\boldsymbol{\lambda}$ and $\boldsymbol{\lambda}'$ differ by 1 so are incongruent modulo $q-1$, monomials of these two types afford distinct characters. Linear independence of characters then shows that any $k\mathbb{F}_q^\times I$-submodule of E contains both the $\boldsymbol{\lambda}$-component and $\boldsymbol{\lambda}'$-component of each of its elements. By hypothesis $\lambda'_0 \neq 0$, so there existis a basic monomial $m = x_1^{a_1} g$ of type $\boldsymbol{\lambda}'$, in which the degree of x_1 has p-adic expression $a_1 = b_{10} + b_{11}p + \cdots + b_{1(t-1)}p^{t-1}$, with $b_{10} \neq 0$. Let $\overline{m} \in E/U$ be its image. Suppose that a $k\mathrm{AGL}(V)$-submodule of E is not contained in U. Then since $E/U \cong S(\boldsymbol{\lambda}')$, it follows that the submodule contains an element mapping to $\overline{m}$ and so by linear independence of characters the submodule contains the image in E of m. We are therefore reduced to proving that the $k\mathrm{AGL}(V)$-submodule of E generated by the image of m contains an element with a nonzero $\boldsymbol{\lambda}$-component. We apply the substitution $\tau : x_1 \mapsto x_1 + 1$, with all other variables left fixed. Then $\tau(m) = m + b_{10}x_1^{a-1}g$, of which the last term is of type $\boldsymbol{\lambda}$, so the proof is complete. □

Remark 13. Let $\leqslant$ denote the ordering on $\mathcal{T}$ induced by the standard ordering of $\mathbb{Z}^t$. By Lemma 12 $\boldsymbol{\lambda} \leqslant \boldsymbol{\lambda}'$ implies $\boldsymbol{\lambda} \preceq \boldsymbol{\lambda}'$, while Lemma 11 shows for example, in the case $t = 2$ that $(0,1) \preceq (p,0)$.

Recall the definition (7) of the lattice M. As noted in Remark 13 the ordering on $\mathcal{T}$ is a refinement of the standard ordering. Theorem 7 predicts that this should be reflected in $\mathcal{D}$ by the presence of positive elements of M which are not non-negative combinations of the $\mathbf{v}_j$. Equation (3) provides some examples of these positive elements. The following lemma can be interpreted as saying that (3) accounts for the existence of all such positive elements.

Lemma 14. *Each element y of $M \cap \mathbb{Z}_+$ can be written in the form*

$$y = \sum_{j=0}^{t-1} a_j(q-1)\mathbf{e}_j + b_j\mathbf{v}_j, \tag{13}$$

with $a_j \geqslant 0$ and $0 \leqslant b_j \leqslant p-1$.

Proof. It follows from (3) that $(q-1)\mathbb{Z}^t \leqslant M$ and that $M/(q-1)\mathbb{Z}^t$ is cyclic of order $q-1$, generated by the image of any $\mathbf{v}_i$. Therefore, the element y is congruent mod $(q-1)\mathbb{Z}^t$ to $b\mathbf{v}_0$, with $0 \leqslant b \leqslant q-2$. Let $b = \sum_{j=0}^{t-1} b_j p^j$ with $0 \leqslant b_j \leqslant p-1$. From (3) we obtain that $p^j \mathbf{v}_0 = \mathbf{v}_j \bmod (q-1)\mathbb{Z}^t$. Thus, we may write

$$y = \sum_{j=0}^{t-1} a_j(q-1)\mathbf{e}_j + b_j \mathbf{v}_j. \tag{14}$$

Then since $y \in \mathbb{Z}_+^t$, by considering the entries in each coordinate of y in (14) we see that $a_j \geqslant 0$ for all j. □

Lemma 15. *Let* $\Phi(\boldsymbol{\lambda}) = \mathbf{d}$ *and* $\Phi(\boldsymbol{\lambda}') = \mathbf{d}'$. *If* $\mathbf{d} \leqslant \mathbf{d}'$ *then* $\boldsymbol{\lambda} \preceq \boldsymbol{\lambda}'$.

Proof. By Lemmas 14 and 11 and proceeding inductively, we are reduced to the case $\mathbf{d}' = \mathbf{d} + \mathbf{v}_j$. This means that if $\boldsymbol{\lambda} = (\lambda_0, \ldots, \lambda_j, \ldots, \lambda_{t-1})$ then $\boldsymbol{\lambda}' = (\lambda_0, \ldots, \lambda_j + 1, \ldots, \lambda_{t-1})$. So Lemma 12 applies. □

4.2 Proofs of theorems

Theorem 7 is immediate from Lemma 15 and the order-preserving property of the bijection Φ. We turn to Theorem 9. Let m be a basic monomial of type $\boldsymbol{\lambda}$. Then $m \in Y_{\Phi(\boldsymbol{\lambda})}$ and has non-zero image in $Y_{\Phi(\boldsymbol{\lambda})}/Y_{<\Phi(\boldsymbol{\lambda})}$. Therefore the submodule generated by m has $S(\boldsymbol{\lambda})$ as a composition factor. Therefore it also has as a composition factor all $S(\boldsymbol{\lambda}')$ with $\boldsymbol{\lambda}' \preceq \boldsymbol{\lambda}$, which by Theorem 7 are all of the composition factors of $Y_{\Phi(\boldsymbol{\lambda})}$. This proves (a). Part (b) follows from Theorem 7 and Corollary 5. We prove (c) by contradiction. Suppose a submodule N of $k[V]$ has $S(\boldsymbol{\lambda})$ as a composition factor, but $N \cap Y_{\Phi(\lambda)} \lneq Y_{\Phi(\lambda)}$. Then by (b), $S(\boldsymbol{\lambda})$ is not a composition factor of $N \cap Y_{\Phi(\lambda)}$ and must therefore be a composition factor of both summands of $(N/N \cap Y_{\Phi(\lambda)}) \oplus (Y_{\Phi(\lambda)}/N \cap Y_{\Phi(\lambda)}) \cong (N + Y_{\Phi(\lambda)})/N \cap Y_{\Phi(\lambda)}$, contrary to the fact that J is multiplicity-free.

To prove (d), let

$$y = \sum \alpha_m m \quad \alpha_m \neq 0 \tag{15}$$

be a linear combination of basic monomials. Let $\mathcal{T}_y \subset \mathcal{T}$ be the set of types in the expression (15) and let $\mathcal{T}_y^*$ be the maximal members of this set with respect to $\preceq$. Next consider the $k\mathrm{AGL}(V)$-submodule Y generated by y. We have

$$Y \leqslant \sum_{\boldsymbol{\mu} \in \mathcal{T}_y} Y_{\Phi(\boldsymbol{\mu})} = \sum_{\boldsymbol{\mu} \in \mathcal{T}_y^*} Y_{\Phi(\boldsymbol{\mu})}. \tag{16}$$

Let $\boldsymbol{\mu} \in \mathcal{T}_y^*$. Then maximality of $\boldsymbol{\mu}$ implies that there is a nonzero homomorphism from $\sum_{\boldsymbol{\mu} \in \mathcal{T}_y^*} Y_{\Phi(\boldsymbol{\mu})}$ to $S(\boldsymbol{\mu})$ such that every basic monomial of different type from $\boldsymbol{\mu}$ mapped to

zero, while the images of basic monomials of type $\boldsymbol{\mu}$ form a basis of $S(\boldsymbol{\mu})$. In particular, the image of y is not zero. Therefore $S(\boldsymbol{\mu})$ is a composition factor of Y. Then (b) implies that $Y_{\Phi(\mu)} \leqslant Y$. Since this holds for each $\boldsymbol{\mu} \in \mathcal{T}_y^*$, we have equality in (16). □

5 Supplementary results

In this final section we include several observations which are closely related to our main discussion but not central to it. They are based on very well known material and do not require the main theorems.

5.1 The radical and socle series of $k[V]$

The *socle* of a module M, denoted $\mathrm{soc}(M)$, is the sum of all simple submodules or, equivalently, the maximal semisimple submodule. The *radical*, $\mathrm{rad}(M)$, is the intersection of all maximal submodules or, equivalently, the smallest submodule by which the quotient module is semisimple. The higher radicals and socles are defined recursively in the usual way: $\mathrm{soc}^i(M)$ is the full preimage in M of $\mathrm{soc}(M/\mathrm{soc}^{i-1}(M))$ and $\mathrm{rad}^i(M) = \mathrm{rad}(\mathrm{rad}^{i-1}(M))$. The *radical length* $\ell(M)$ is the smallest index i such that $\mathrm{rad}^i(M) = 0$. Thus, the socle series is an ascending chain of submodules with semisimple quotients and the radical series is a descending chain with semisimple quotients. The radical series and socle series are said to be equal if they are the same as sets of subspaces, namely $\mathrm{rad}^{\ell(M)-i}M = \mathrm{soc}^i M$.

Theorem 16. *The radical and socle series of $k[V]$ with respect to $k\mathrm{AGL}(V)$ are equal. The socle length is $N = nt(p-1)+1$ and the i-th socle layer is isomorphic to*

$$\bigoplus_{|\boldsymbol{\lambda}|=i-1} S(\boldsymbol{\lambda}), \tag{17}$$

where $|\boldsymbol{\lambda}| = \lambda_0 + \cdots + \lambda_{t-1}$.

Since Theorem 7 completely describes the submodule lattice of $k[V]$, the socle and radical series of any submodule can be found directly from this result. Thus, Theorem 16 is just one example. However, Theorem 16 does not require the full strength of Theorem 7 and it may be instructive to see how it can be deduced from the classical prime field case $t = 1$.

The restriction of $k[V]$ to the subgroup V is isomorphic to the regular module for V. Let $\mathrm{soc}_V^i(k[V])$ denote its i-th socle and $\mathrm{rad}_V^i(k[V])$ its i-th radical.

Assume now that we are in the prime field case. For $0 \leqslant r \leqslant n(p-1)$, the *$r$-th order p-ary Generalized Reed-Muller code* is simply the subspace F_r in the degree filtration. We set $F_{-1} = 0$. It is a well known fact, first proved in [2], that this family of subcodes of $k[V]$ is equal to the socle and radical series with respect to V. (See [4] for the history, a proof and generalizations, [16, 7.2] for further discussion and references.) We present here a self-contained proof of this fact.

Lemma 17. *For $0 \leqslant i \leqslant n(p-1)+1$ we have*

$$\mathrm{soc}_V^i(k[V]) = F_{i-1} = \mathrm{rad}_V^{n(p-1)+1-i}(k[V]). \tag{18}$$

Proof. The action of V on $k[V]$ is by translation of functions. In coordinates, let $f = f[x_1, \ldots, x_n]$ be written in terms of the monomial basis, let d be its degree and let $u = -(a_1, \ldots, a_n)$. Then we have a "Taylor expansion"

$$\begin{aligned}(uf)(x_1, \ldots, x_n) &= f(x_1 + a_1, \ldots, x_n + a_n) \\ &= f(x_1, \ldots, x_n) + \sum_i a_i \frac{\partial f}{\partial x_i} + \text{ terms of degree} \leqslant d-2\ ,\end{aligned} \tag{19}$$

It is immediate from (19) that for $0 \leqslant r \leqslant n(p-1)$, the subspace F_r is a kV-submodule of $k[V]$ and that V acts trivially on each quotient F_r/F_{r-1}. In order to prove the first equality of the lemma, it suffices to show that the module F_r/F_{r-1} is the whole socle, that is the set of all fixed points, of the module $k[V]/F_{r-1}$. In other words, we must prove that if $f \in k[V]$ has degree $d \geqslant r+1$ then there exists $u \in V$ such that $uf - f \neq 0 \bmod F_{r-1}$. It will be enough if $uf - f \neq 0 \bmod F_{d-2}$. Without loss of generality, we can assume the variable x_1 occurs in f. The desired conclusion is then read off from (19) by setting $u = (1, 0, \ldots, 0)$ and recalling that the partial degree of f in x_1 is $\leqslant p-1$.

The argument to prove the second equality is dual in some sense. It suffices to prove that the elements $uf - f$ for $f \in F_r$ and $u \in V$ generate F_{r-1}. This will follow if we show that each basis monomial of degree $\leqslant r-1$ is of the form $uf - f$ for some element $f \in F_r$ and some $u \in V$. Since $r - 1 < n(p-1)$, at least one variable in such a monomial has exponent $< p-1$ and so by (19) we obtain f by partial integration. □

Proof of Theorem 16

$\mathrm{AGL}(V)$ acts on the kV-socle series and from Lemma 17 we see that the subquotient $\mathrm{soc}_V^i(k[V])/\mathrm{soc}_V^{i-1}(k[V])$ is isomorphic to the simple $k\mathrm{AGL}(V)$-module $\overline{S}^{i-1}(V \otimes_{\mathbb{F}_p} k)$. Since V acts trivially on any semisimple $k\mathrm{AGL}(V)$-module, it follows that the kV-socle series is also equal (as sets of subspaces) to the $k\mathrm{AGL}(V)$-socle series and radical series (and incidentally that $k[V]$ is a uniserial $k\mathrm{AGL}(V)$-module). Thus, Theorem 16 holds in the case $t = 1$.

Returning now to the general case, we can place ourselves in the prime case if we forget the $\mathbb{F}_q$-structure of V and regard it as an nt-dimensional $\mathbb{F}_p$-vector space, which we denote by $V_{\mathbb{F}_p}$ when necessary. Then we apply the prime field case to the nt-dimensional affine group $\mathrm{AGL}(V_{\mathbb{F}_p})$. Thus, we have a $k\mathrm{AGL}(V_{\mathbb{F}_p})$-isomorphism

$$\mathrm{soc}_V^i(k[V])/\mathrm{soc}_V^{i-1}(k[V]) \cong \overline{S}^{i-1}(V \otimes_{\mathbb{F}_p} k), \quad (1 \leqslant i \leqslant nt(p-1)+1). \tag{20}$$

We next compute the restriction of this module to $\mathrm{AGL}(V)$. As $k\mathrm{AGL}(V)$-modules, we have

$$V \otimes_{\mathbb{F}_p} k \cong \bigoplus_{j=0}^{t-1} V_k^{(p^j)}. \tag{21}$$

At this point, we shall need some general facts about truncated polynomial rings. For any vector space W over k let $\overline{S}(W^*)$ denote the quotient of the symmetric algebra $S(W^*)$ of W^* by the ideal generated by all elements f^p for $f \in W^*$. This is simply a coordinate-free description of the truncated polynomial algebra $k[y_1, \ldots, y_r]/(y_1^p, \ldots, y_r^p)$, where the y_i are coordinate functions on W. We claim that for two vector spaces V_1 and V_2, we have a canonical isomorphism of graded algebras

$$\overline{S}(V_1^*) \otimes \overline{S}(V_2^*) \cong \overline{S}(V_1^* \oplus V_2^*).$$

We start from the familiar case of symmetric algebras, where we have a canonical isomorphism of graded algebras

$$S(V_1^*) \otimes S(V_2^*) \cong S(V_1^* \oplus V_2^*)$$

defined by multiplication. The inverse map is defined by applying the universal mapping property of $S(V_1^* \oplus V_2^*)$ to the linear map $V_1^* \oplus V_2^* \to S(V_1^*) \otimes S(V_2^*)$ sending (f, g) to $f \otimes 1 + 1 \otimes g$. It is immediate that the ideal generated by p-th powers in $S(V_1^* \oplus V_2^*)$ corresponds under these isomorphisms to the ideal of $S(V_1^*) \otimes S(V_2^*)$ generated by the elements $f^p \otimes 1$ and $1 \otimes g^p$, for $f \in V_1^*$ and $g \in V_2^*$. Thus, we have induced inverse isomorphisms of the truncated algebras as claimed. The canonical nature of these isomorphisms ensures that they are equivariant with respect to the induced group action if V_1 and V_2 are modules for some group.

We now apply these observations to the decomposition (21). In degree $i-1$, we obtain the isomorphism

$$\overline{S}^{i-1}(V \otimes_{\mathbb{F}_p} k) \cong \bigoplus_{\substack{0 \leqslant \lambda_j \leqslant n(p-1) \\ \lambda_0 + \cdots + \lambda_{t-1} = i-1}} \overline{S}^{\lambda_0}(V_k) \otimes \overline{S}^{\lambda_1}(V_k^{(p)}) \otimes \cdots \overline{S}^{\lambda_{t-1}}(V_k^{(p^{t-1})}). \tag{22}$$

In particular, this shows that $\mathrm{soc}_V^i(k[V])/\mathrm{soc}_V^{i-1}(k[V])$ is a semsisimple $k\mathrm{AGL}(V)$-module, which implies that the socle and radical series of $k[V]$ with respect to $k\mathrm{AGL}(V)$ are the same as the series with respect to kV. Since (22) also gives the composition factors of the socle layers, the proof of Theorem 16 is complete. □

Our proof of Theorem 16 contains the following additional information.

Corollary 18. *The radical and socle series of the module $k[V]$ are equal to each other and the same (as sets of k-subspaces) whether $k[V]$ is regarded as a $k\mathrm{AGL}(V)$-module or as the regular kV-module. In particular, the radical and socle series are independent of the field over which V is taken to be a vector space.*

□

5.2 Change of scalars

For completeness, we will give the general formulation for the change of fields involved in the preceding subsection. Let u be a divisor of t and set $v = t/u$. When necessary, we will use the notation $V_{\mathbb{F}_{p^u}}$ when we wish to consider V as an nv-dimensional vector space over $\mathbb{F}_{p^u}$. The types of the composition factors of $k[V]$ with respect to $\mathrm{AGL}(V_{\mathbb{F}_{p^u}})$ (or, equivalently, $\mathrm{GL}(V_{\mathbb{F}_{p^u}})$ since V acts trivially) are u-tuples $\boldsymbol{\rho} = (\rho_0, \ldots, \rho_{u-1})$ with $0 \leqslant \rho_\ell \leqslant nv(p-1)$. We will modify the notation of section 3.2 slightly by calling these $\mathbb{F}_{p^u}$-types and denoting the corresponding simple modules by $S_{\mathbb{F}_{p^u}}(\boldsymbol{\rho})$. We keep the previous notation for the case $u = t$.

Our aim is to describe the restriction of $S_{\mathbb{F}_{p^u}}(\rho_0, \ldots, \rho_{u-1})$ to $\mathrm{GL}(V)$. Given a $\mathbb{F}_{p^u}$-type $\boldsymbol{\rho} = (\rho_0, \ldots, \rho_{t-1})$ we consider the set the set of all $u \times v$ matrices with entries $\lambda_{\ell m}$, $(0 \leqslant \ell \leqslant u-1,\ 0 \leqslant m \leqslant v-1)$, satisfying:

1. $0 \leqslant \lambda_{\ell m} \leqslant n(p-1)$;

2. For each ℓ, the sum of the entries in the ℓ-th row equals ρ_ℓ.

We obtain an $\mathbb{F}_q$-type from each such matrix by listing the t matrix entries starting from the top left and moving down successive columns. Thus $\lambda_{\ell m}$ is the $um + \ell$ entry of the $\mathbb{F}_q$-type. Let $\mathcal{T}(\boldsymbol{\rho})$ be the set of types obtained in this way.

Theorem 19. *As $k\mathrm{GL}(V)$-modules, we have*

$$S_{\mathbb{F}_{p^u}}(\rho_0, \ldots, \rho_{u-1}) \cong \bigoplus_{\boldsymbol{\lambda} \in \mathcal{T}(\boldsymbol{\rho})} S(\boldsymbol{\lambda}). \tag{23}$$

Proof. The result follows from the definitions and the additive properties of tensor products, together with the following straightforward generalization of (22). For $0 \leqslant \rho \leqslant nv(p-1)$, we have

$$\overline{S}^{\rho}(V \otimes_{\mathbb{F}_{p^u}} k) \cong \bigoplus_{\substack{0 \leqslant \lambda_j \leqslant n(p-1) \\ \lambda_0 + \cdots + \lambda_{v-1} = \rho}} \overline{S}^{\lambda_0}(V_k) \otimes \overline{S}^{\lambda_1}(V_k^{(p^u)}) \otimes \cdots \overline{S}^{\lambda_{v-1}}(V_k^{(p^{(t-u)})}). \tag{24}$$

□

References

[1] M. Bardoe, and 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. Lond. Math. Soc.*, 61:58–80, 2000.

[2] P. Charpin. Codes idéaux de certaines algèbres modulaires. *Thèse de 3ième cycle*, Université VII, Paris, 1982.

[3] P. Charpin. Codes cycliques étendus affines-invariants et antichaines d'un ensemble partiellement ordonnée. *C. R. Acad. Sci. Paris Ser. I Math.*, 302(5):171–174, 1986.

[4] P. Charpin. Une généralisation de la construction de Reed et Muller p-aires. *Comm. Algebra*, 16: 2231–2246, 1988.

[5] P. Charpin. Codes cycliques étendus affines-invariants et antichaines d'un ensemble partiellement ordonnée. *Discrete Math.*, 80(3):229–247, 1990.

[6] P. Delsarte. On cyclic codes that are invariant under the general linear group, *IEEE Trans. Information Theory*, IT-16(6):760–769, 1970.

[7] P. Delsarte, J. M. Goethals, and F. S. MacWilliams. On generalized Reed-Muller codes and their relatives. *Information and Control*, 16:403–442, (1970).

[8] S. Doty. The symmetric algebra and representations of general linear groups. *Proceedings of the Hyderabad Conference on Algebraic Groups* 123–150, 1989.

[9] J. C. Jantzen. *Representations of Algebraic Groups.* Academic Press, London, 1987.

[10] T. Kasami, S. Lin, and W. W. Peterson. Some results on cyclic codes which are invariant under the affine group and their applications. *Information and Control*, 11:475–496, 1967.

[11] L. G. Kovacs. Some representations of special linear groups. *Proc. Symposia in Pure Math.*, 47(2):207–218, 1987.

[12] L. Krop. On comparison of M-, G- and S-representations. *J. Algebra*, 146: 497–513, 1992.

[13] N. Kuhn. Invariant subspaces of the ring of functions on a vector space over a finite field. *J. Algebra* 191(2):212–227, 1997.

[14] F. J. MacWilliams, and N. J. A. Sloane. *The theory of error-correcting codes I, II.* North-Holland Mathematical Library, Vol. 16. North-Holland, Amsterdam, 1977.

[15] B. Mortimer. The modular permutation representations of the known doubly transitive groups. *Proc. London Math.Soc.*, 41:1–20, 1980.

[16] W. Willems. *Codierungstheorie.* Walter de Gruyter, Berlin, 1999.