INVARIANTS OF POLYNOMIALS MOD FROBENIUS POWERS

C. DRESCHER AND A. V. SHEPLER

Abstract. Lewis, Reiner, and Stanton conjectured a Hilbert series for a space of invariants under an action of finite general linear groups using (q,t)-binomial coefficients. This work gives an analog in positive characteristic of theorems relating various Catalan numbers to the representation theory of rational Cherednik algebras. They consider a finite general linear group as a reflection group acting on the quotient of a polynomial ring by iterated powers of the irrelevant ideal under the Frobenius map. We prove a variant of their conjecture in the local case, when the group acting fixes a reflecting hyperplane.

1. Introduction

In 2017, Lewis, Reiner and Stanton [9] conjectured a combinatorial formula for the Hilbert series of a space of invariants under the action of the general linear group $\mathrm{GL}_n(\mathbb{F}_q)$ over a finite field $\mathbb{F}_q$ in terms of (q,t)-binomial coefficients. This formula provides an analogue for the q-Catalan and q-Fuss Catalan numbers which connect Hilbert series for certain invariant spaces with the representation theory of rational Cherednik algebras for Coxeter and complex reflection groups. Results in the theory of reflection groups often follow from a local argument after considering the subgroup fixing one reflecting hyperplane. We prove here a version of the conjecture in the local case. We expect this local theory will extend to one for any modular reflection group, including $\mathrm{GL}_n(\mathbb{F}_q)$.

Lewis, Reiner, and Stanton consider $\mathrm{GL}_n(\mathbb{F}_q)$ acting on $V=(\mathbb{F}_q)^n$ and the polynomial ring $S=S(V^*)=\mathbb{F}_q[x_1,\ldots,x_n]$ by transformation of variables $x_1,\ldots,x_n$ in V^*. They consider the quotient of S by the m-th iterated Frobenius power of the irrelevant ideal,

$$\mathfrak{m}^{[q^m]} := (x_1^{q^m},\ldots,x_n^{q^m})\,,$$

which we call the *Frobenius irrelevant ideal.* Their conjecture gives the Hilbert series for the $\mathrm{GL}_n(\mathbb{F}_q)$-invariants in $\mathbb{F}_q[x_1,\ldots,x_n]/(x_1^{q^m},\ldots,x_n^{q^m})$ using (q,t)-binomial coefficients.

We consider subgroups of reflections about a single hyperplane H in V. These groups are not cyclic in general, in contrast to groups over fields of characteristic zero. We first take the case when q is a prime p and then generalize some of our ideas to arbitrary q. We explicitly describe the space of G-invariants in $S/\mathfrak{m}^{[p^m]}$ for any subgroup $G\subset \mathrm{GL}_n(\mathbb{F}_p)$ fixing a hyperplane H in V pointwise. We give the Hilbert series in terms of the dimension of the transvection root space. We then describe the invariants under the full pointwise stabilizer $\mathrm{GL}_n(\mathbb{F}_q)_H$ in $\mathrm{GL}_n(\mathbb{F}_q)$ of any hyperplane H for q a prime power:

Date: April 2, 2020.

Key words and phrases. reflection groups, invariant theory, Catalan numbers, Fuss-Catalan numbers, Frobenius map, (q,t)-binomial coefficients, transvections.

The second author was partially supported by Simons grant 429539.

Theorem 1.1. *For any hyperplane H in $V = \mathbb{F}_q^n$,*

$$\mathrm{Hilb}\left(\left({S}/{\mathfrak{m}^{[q^m]}}\right)^{\mathrm{GL}_n(\mathbb{F}_q)_H},\ t\right) = ([q^{m-1}]_{t^q})^{n-1}\begin{bmatrix} m \\ 1 \end{bmatrix}_{q,t} + t^{q^m-1}([q^m]_t)^{n-1}\begin{bmatrix} m \\ 0 \end{bmatrix}_{q,t}.$$

Recall the q-integer $[m]_q = 1+q+q^2+\ldots+q^{m-1}$ and (q,t)-binomial coefficient (see [11])

$$\begin{bmatrix} m \\ k \end{bmatrix}_{q,t} := \prod_{i=0}^{k-1} \frac{1-t^{q^m-q^i}}{1-t^{q^k-q^i}}.$$

We compare with the Lewis, Reiner, Stanton conjecture in Section 2 and give this Hilbert series in terms of q-Fuss Catalan numbers. The conjecture implies that the dimension over $\mathbb{F}_q$ of the $\mathrm{GL}_n(\mathbb{F}_q)$-invariants in $S/\mathfrak{m}^{[q^m]}$ counts the number of orbits in $(\mathbb{F}_{q^m})^n$ under the action of $\mathrm{GL}_n(\mathbb{F}_q)$ and that this dimension is $\sum_{k=0}^{\min(n,m)} \begin{bmatrix} m \\ k \end{bmatrix}_q$ (see [9, Section 7.1 and Theorem 6.16]). We prove an analogous statement in Section 9:

Corollary 1.2. *For any hyperplane H in $V = (\mathbb{F}_q)^n$, the number of orbits in $(\mathbb{F}_{q^m})^n$ under the action of $\mathrm{GL}_n(\mathbb{F}_q)_H$ is*

$$\dim_{\mathbb{F}_q}\left({S}/{\mathfrak{m}^{[q^m]}}\right)^{\mathrm{GL}_n(\mathbb{F}_q)_H} = q^{(m-1)(n-1)}\begin{bmatrix} m \\ 1 \end{bmatrix}_q + q^{m(n-1)}\begin{bmatrix} m \\ 0 \end{bmatrix}_q.$$

Example 1.3. Consider G acting on $V = (\mathbb{F}_5)^3$ with $\dim_{\mathbb{F}_5}(\mathrm{RootSpace}(G) \cap H) = 2$. Then G is generated by two transvections and possibly a diagonalizable reflection. We may assume (after a change-of-basis) that

$$G = \left\langle \begin{pmatrix} 1&0&0\\0&1&0\\0&0&\omega \end{pmatrix}, \begin{pmatrix} 1&0&1\\0&1&0\\0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0\\0&1&1\\0&0&1 \end{pmatrix} \right\rangle$$

for some primitive e-th root-of-unity ω in $\mathbb{F}_5$. The m-th iterated irrelevant ideal in $\mathbb{F}_5[x_1, x_2, x_3]$ is $(x_1^{5^m}, x_2^{5^m}, x_3^{5^m})$ for $m \geq 1$. We will see in Section 7 that

$$\mathrm{Hilb}\left(\left({S}/{\mathfrak{m}^{[5^m]}}\right)^G,\ t\right) = \frac{(1-t^{5^m})^2}{(1-t^5)^2(1-t^e)}\left(1 - t^{5^m-1} + t^{5^m-1}(1-t^e)\left(\frac{1-t^5}{1-t}\right)^2\right).$$

Outline. In Section 2, we give motivation from the theory of rational Catalan combinatorics, which relates rational Cherednik algebras with various kinds of Catalan numbers. We recall some facts on modular reflection groups in Section 3. In Sections 4 to 7, we mainly consider a subgroup G of $\mathrm{GL}_n(\mathbb{F}_p)$ fixing a hyperplane H with maximal transvection root space; more general results in Sections 6 and 8 will follow from this special case. We give a Groebner basis for $S^G \cap \mathfrak{m}^{[p^m]}$ in Section 4 and compute the Hilbert series for $S^G/(S^G \cap \mathfrak{m}^{[p^m]})$ in Section 5. In Section 6, we decompose $(S/\mathfrak{m}^{[p^m]})^G$ as the direct sum of $S^G/(S^G \cap \mathfrak{m}^{[p^m]})$ and a complement. We give the Hilbert series for the G-invariants in $S/\mathfrak{m}^{[p^m]}$ when G has maximal root space in Section 7 and for general groups fixing a hyperplane over $\mathbb{F}_p$ in Section 8. We consider the full pointwise stabilizer of a hyperplane in $\mathrm{GL}_n(\mathbb{F}_q)$ in Section 9: We establish Theorem 1.1 and show the Hilbert series counts orbits. We give a bound on the Hilbert series for $\mathrm{GL}_n(\mathbb{F}_q)$ in the conjecture of Lewis, Reiner, and Stanton in Section 10. Lastly, in Section 11, we give a resolution directly for $S^G \cap \mathfrak{m}^{[p^m]}$ in the 2-dimensional case.

2. Motivation

We recall some motivation for studying the invariants of $S/\mathfrak{m}^{[q^m]}$ from the theory of Catalan combinatorics for Coxeter and complex reflection groups; see Armstrong, Reiner, and Rhoades [1]; Berest, Etingof and Ginzburg [2]; Bessis and Reiner [3]; Gordon [5]; Gordon and Griffeth [6]; Krattenthaler and Müller [8]; and Stump [13].

Graded Parking Spaces and Rational Cherednik Algebras. The parking space of an irreducible Weyl group gives an irreducible representation of the associated rational Cherednik algebra. The q-Catalan number for the group records the Hilbert series for the invariants in this space in terms of the degrees $d_1, \dots, d_n$ and Coxeter number h (see [6]) of the reflection group. More generally, for an irreducible Coxeter group W acting on $V = \mathbb{C}^n$, the graded parking space representation (see [1]) is isomorphic to $S/(\theta_1, \dots, \theta_n)$ for some homogeneous polynomials $\theta_1, \dots, \theta_n$ in S of degree $h+1$ with $\mathbb{C}\text{-span}\{\theta_1, \dots, \theta_n\}$ isomorphic to the reflection representation V^*. The W-invariants in the parking space has Hilbert series given by the q-Catalan number for W:

$$\mathrm{Hilb}\left(\left({}^{S}\!\big/\!_{(\theta_1, \dots, \theta_n)}\right)^W,\ q\right) = \mathrm{Cat}(W, q) = \prod_{i=1}^{n} \frac{1-q^{h+d_i}}{1-q^{d_i}}\,.$$

For a complex reflection group W, Gordon and Griffeth [6] connect the representation theory of the associated rational Cherednik algebra to the m-th q-Fuss Catalan numbers,

$$\mathrm{Cat}^{(m)}(W, q) = \prod_{i=1}^{n} \frac{[d_i + mh]_q}{[d_i]_q} \;=\; \prod_{i=1}^{n} \frac{1-q^{d_i+mh}}{1-q^{d_i}}\ ,$$

giving the Hilbert series of W-invariants in a space $S/(\tilde{\theta}_1, \dots, \tilde{\theta}_n)$ with $\deg(\tilde{\theta}_i) = mh+1$.

Lewis, Reiner, and Stanton Conjecture. The ideal $(\theta_1, \dots, \theta_n)$ takes a particularly nice form for some Coxeter groups with $\theta_i = x_i^{h+1}$; the graded parking space in this case is just $\mathbb{C}[x_1, ..., x_n]/(x_1^{h+1}, \dots, x_n^{h+1})$. Lewis, Reiner, and Stanton [9] ask what ideal can play the role of $(\theta_1, \dots, \theta_n)$ for the modular reflection group $\mathrm{GL}_n(\mathbb{F}_q)$. They consider the ideal $(\theta_1, \dots, \theta_n) = (x_1^{q^m}, \dots, x_n^{q^m}) = \mathfrak{m}^{[q^m]}$ for $m \geq 0$ since $\theta_1, \dots, \theta_n$ span a $\mathrm{GL}_n(\mathbb{F}_q)$-stable subspace over $\mathbb{F}_q$ with the map $x_i \mapsto x_i^{q^m}$ defining a $\mathrm{GL}_n(\mathbb{F}_q)$-equivariant isomorphism (see [9]). The quotient $S/\mathfrak{m}^{[q^m]}$ is $(q^m)^n$-dimensional, and Lewis, Reiner, and Stanton give a conjecture for the Hilbert series of its $\mathrm{GL}_n(\mathbb{F}_q)$-fixed subspace:

Conjecture 2.1 ([9]). *The space of $\mathrm{GL}_n(\mathbb{F}_q)$-invariants in ${}^{S}\!\big/\!_{\mathfrak{m}^{[q^m]}}$ has Hilbert series*

$$\begin{aligned}\mathrm{Hilb}\left(\left({}^{S}\!\big/\!_{\mathfrak{m}^{[q^m]}}\right)^{\mathrm{GL}_n(\mathbb{F}_q)},\ t\right) &= \sum_{k=0}^{\min(n,m)} t^{(n-k)(q^m-q^k)} \begin{bmatrix} m \\ k \end{bmatrix}_{q,t} \\ &= \sum_{k=0}^{\min(n,m)} t^{(n-k)(q^m-q^k)} \frac{\mathrm{Hilb}(S^{P_k}, t)}{\mathrm{Hilb}(S^{\mathrm{GL}_m(\mathbb{F}_q)}, t)}\end{aligned}$$

for P_k the maximal parabolic subgroup of $\mathrm{GL}_m(\mathbb{F}_q)$ stabilizing any $\mathbb{F}_q$-subspace of $(\mathbb{F}_q)^m$ isomorphic to $(\mathbb{F}_q)^k$.

Compare with our Theorem 1.1, which is equivalent to the statement that

$$\mathrm{Hilb}\left(\left(S/\mathfrak{m}^{[q^m]}\right)^{\mathrm{GL}_n(\mathbb{F}_q)_H},\ t\right) \;=\; \frac{\mathrm{Hilb}(S^{\mathrm{GL}_n(\mathbb{F}_q)_H}, t)}{\mathrm{Hilb}(S^{\mathrm{GL}_n(\mathbb{F}_{q^m})_H}, t)} \;+\; \frac{(t^{q^m-1}-t^{q^m})}{(1-t^{q^m-1})}\,\frac{\mathrm{Hilb}(S,\ t)}{\mathrm{Hilb}(S^{\mathrm{GL}_n(\mathbb{F}_{q^m})_H}, t)}\,.$$

A curious reformulation. We mention a version of Theorem 1.1 in terms of q-Fuss Catalan numbers that connects with Conjecture 2.1; we wonder if a version of this reformulation holds for other reflection groups. For modular reflection groups, the above definition of Coxeter number does not always give an integer, so we use an alternate definition that agrees with the traditional one over $\mathbb{R}$ or $\mathbb{C}$. For any reflection group G acting on V with a polynomial ring of invariants $S^G = \mathbb{F}[f_1, \ldots, f_n]$, define the

$$\textit{Coxeter number of } G := \frac{\deg J + \deg Q}{n}$$

for $J = \det\{\partial f_i/\partial x_j\}_{i,j=1,\ldots,n}$ in S, the determinant of the Jacobian derivative matrix, and $Q = \prod_{H\in\mathcal{A}} l_H$, the polynomial in S defining the arrangement $\mathcal{A}$ of reflecting hyperplanes for G. Note that $\deg J$ is *not* the number of reflections in G in general.

For any hyperplane H in $V = \mathbb{F}_q^n$ and $G = \mathrm{GL}_n(\mathbb{F}_q)_H$, Theorem 1.1 implies that

$$\mathrm{Hilb}\left(\left(S/\mathfrak{m}^{[q^m]}\right)^{G},\ t\right) \;=\; \sum_{k=0,1} t^{(n-\dim G_k)(q^m-q^k)}\ \mathrm{Cat}^{(c_k)}(G_k, t) \tag{2.2}$$

where $c_k = (q^m - q^k)/h_k$ and $G_k = \big(\mathrm{Stab}_G(V_k)\big)|_{V_k}$ (setwise stabilizer) with Coxeter number h_k for $V_0 = H$ and $V_1 = V$. Here, G_0 is the identity subgroup of $\mathrm{GL}_{n-1}(\mathbb{F}_q)$ regarded as the direct sum of trivial reflection groups with degrees $1, \ldots, 1$ and Coxeter number 1 while $G_1 = G$ has Coxeter number $q-1$. Each Fuss parameter c_k lies in $\mathbb{N}$ although G_k is reducible.

Although reformulation Eq. (2.2) is somewhat artificial, it agrees with a version of the Lewis, Reiner, and Stanton conjecture if we allow for non-integer Fuss parameters. For $G = \mathrm{GL}_n(\mathbb{F}_q)$, Conjecture 2.1 implies that

$$\mathrm{Hilb}\left(\left(S/\mathfrak{m}^{[q^m]}\right)^{G},\ t\right) \;=\; \sum_{k=0}^{\min\{n,m\}} t^{(n-\dim G_k)(q^m-q^k)}\ \mathrm{Cat}^{c_k}(G_k, t)$$

where again $c_k = (q^m - q^k)/h_k$ and $G_k = \big(\mathrm{Stab}_G(V_k)\big)|_{V_k} = \mathrm{GL}_k(\mathbb{F}_q)$ with Coxeter number $h_k = q^k - 1$ for $V_k = (\mathbb{F}_q)^k \subset (\mathbb{F}_q)^n$. Here, at least the groups G_k are irreducible.

3. Reflection groups and transvections

Recall that a *reflection* on $V = \mathbb{F}^n$ for any field $\mathbb{F}$ is a transformation s in $\mathrm{GL}(V)$ whose fixed point space is a hyperplane H in V. A *reflection group* is a subgroup of $\mathrm{GL}(V)$ generated by reflections; we assume all reflection groups are finite. Suppose G is a reflection group fixing a hyperplane H in V and choose some linear form l in V^* defining H, i.e., with $\mathrm{Ker}\, l = H$. Every g in G defines a *root vector* α_g in V satisfying

$$g(v) = v + l(v)\alpha_g \qquad \text{for all } v \text{ in } V\,.$$

We denote the collection of all root vectors by $\mathrm{RootSpace}(G)$. In the *nonmodular setting*, when the characteristic p is relatively prime to $|G|$, the group G is cyclic. In this case, every group element is semisimple, and one can choose a G-invariant inner product so that any root vector for H is perpendicular to H. In the *modular setting*, when $p = \mathrm{char}(\mathbb{F})$ divides $|G|$, the root vector of a reflection g may lie *in H* itself; this occurs exactly when g is not semisimple. Such reflections are called *transvections* and they have order $p = \mathrm{char}(\mathbb{F})$.

The transvections in G form a normal subgroup K, the kernel of the determinant character $\det : G \to \mathbb{F}^\times$. The group G is generated by K and some semisimple element g_n of maximal order $e = |G/K|$, and G is isomorphic to the semi-direct product of K and the cyclic subgroup $\langle g_n \rangle$ of semisimple reflections:

$$G \cong K \rtimes \mathbb{Z}/e\mathbb{Z}\,.$$

Now assume $\mathbb{F} = \mathbb{F}_p$ for a prime p. The corresponding *transvection root space* $\mathrm{RootSpace}(G) \cap H$ is an $\mathbb{F}_p$-vector space (see [7]), and its dimension,

$$\ell = \dim_{\mathbb{F}_p}\left(\mathrm{RootSpace}(G) \cap H\right),$$

is the minimal number of transvections needed to generate G: there are transvections $g_1, \ldots, g_\ell$ with $G = \langle g_1, \ldots, g_\ell, g_n \rangle$ and $|G| = e \cdot p^\ell$.

After conjugation. We may choose a basis $v_1, \ldots, v_n$ of V with dual basis $x_1, \ldots, x_n$ of V^* so that $v_1, \ldots, v_{n-1}$ span the hyperplane $H = \mathrm{Ker}\,(x_n)$, g_n fixes $x_1, \ldots, x_{n-1}$, and $g_n(x_n) = \omega^{-1} x_n$ for ω a primitive e-th root-of-unity in $\mathbb{F}_p$. We furthermore refine the basis so that each transvection g_k fixes $x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n$ and $g_k(x_k) = x_k - x_n$:

$$g_n = \begin{pmatrix} 1 & \ldots & 0 & 0 \\ \vdots & \ddots & & \vdots \\ 0 & \ldots & 1 & 0 \\ 0 & \ldots & 0 & \omega \end{pmatrix} \qquad \text{and, for } 1 \le k \le \ell, \quad g_k := \begin{array}{c} \begin{pmatrix} 1 & \cdots & & & & \cdots & 0 \\ \vdots & \ddots & & & & & \vdots \\ 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 1 \\ 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & & \ddots & \vdots \\ 0 & \cdots & & & & \cdots & 1 \end{pmatrix} \end{array} \begin{array}{l} \\ \\ \\ \leftarrow k^{\text{th}} \text{ row}\,. \\ \\ \\ \\ \end{array}$$

Example 3.1. When $n = 3$, $p = 5$, and $\ell = 1$, G acting on $V = (\mathbb{F}_5)^3$ is generated by one transvection and possibly an additional semisimple reflection. We may assume (after a change-of-basis) that for some e-th root-of-unity ω in $\mathbb{F}_5$

$$G = \left\langle g_3 = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \omega \end{smallmatrix}\right),\ g_1 = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \right\rangle\,.$$

Basic Invariants. The ring of invariant polynomials S^G is itself a polynomial ring, $S^G = \mathbb{F}_p[f_1, \ldots, f_n]$ with homogeneous generators

$$f_1 = x_1^p - x_1 x_n^{p-1}, \ldots, f_\ell = x_\ell^p - x_\ell x_n^{p-1}, \quad f_{\ell+1} = x_{\ell+1}, \ldots, f_{n-1} = x_{n-1}, \quad f_n = x_n^e$$

and

$$\mathrm{Hilb}(S^G, t) = \frac{1}{(1-t^p)^\ell\,(1-t)^{n-\ell-1}\,(1-t^e)}\,.$$

Example 3.2. For $G = \left\langle \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \omega \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right) \right\rangle \subset \mathrm{GL}_3(\mathbb{F}_5)$, the ring S^G is generated by $f_1 = x_1^5 - x_1 x_3^4$, $f_2 = x_2^5 - x_2 x_3^4$ and $f_3 = x_3^e$ as an $\mathbb{F}_5$-algebra for $e = \mathrm{order}(\omega)$. The Hilbert series of S^G is

$$\mathrm{Hilb}(\mathbb{F}_5[x_1, x_2, x_3]^G, t) = \frac{1}{(1-t^5)^2\,(1-t^e)}\,.$$

4. Describing the invariants in the Frobenius irrelevant ideal

We begin by finding the invariants in the Frobenius irrelevant ideal itself, describing $S^G \cap \mathfrak{m}^{[p^m]}$. Throughout this section, we assume G is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ fixing a hyperplane H of $V = \mathbb{F}_p$. The general case will follow from the special case when G has maximal transvection root space, so we assume $\ell = n - 1$. Without loss of generality, we may take a basis $x_1, \ldots, x_n$ for V^* so that $H = \operatorname{Ker} x_n$ and G acts as in Section 3.

Monomial orderings. We consider S as a graded ring with respect to the usual polynomial degree with $\deg x_i = 1$ for all i. The Frobenius irrelevant ideal $\mathfrak{m}^{[p^m]}$ is then a homogeneous ideal giving a graded quotient $S/\mathfrak{m}^{[p^m]}$. We use compatible monomial orderings on the two polynomial rings S and S^G. On $S = \mathbb{F}_p[x_1, \ldots, x_n]$, we take the graded lexicographical ordering with $x_1 > x_2 > \cdots > x_n$. On $S^G = \mathbb{F}_p[f_1, \ldots, f_n]$, we take the inherited graded lexicographical ordering with $\deg(f_n) = e < p$, $\deg(f_i) = p$ for $i < n$, and $f_1 > f_2 > \cdots > f_n$. Then for any polynomials f and f' in S^G, $f < f'$ in the monomial ordering on S^G if and only if $f < f'$ in the monomial ordering on S. We use the notation $\mathrm{LM}_S(f)$ and $\mathrm{LM}_{S^G}(f)$ for the leading monomials of a polynomial f with respect to the ordering on S and S^G, respectively. Then

$$\mathrm{LM}_S\big(\mathrm{LM}_{S^G}(f)\big) = \mathrm{LM}_S(f). \tag{4.1}$$

We will frequently use the fact that for any nonnegative exponents a_i and $i < n$,

$$f_i\, x_1^{a_1} \ldots x_{n-1}^{a_{n-1}}\, x_n^{p^m-1} \equiv x_1^{a_1} \ldots x_{i-1}^{a_{i-1}} x_i^{p+a_i} x_{i+1}^{a_{i+1}} \ldots x_{n-1}^{a_{n-1}}\, x_n^{p^m-1} \mod \mathfrak{m}^{[p^m]}\,. \tag{4.2}$$

Generators for invariants in the Frobenius irrelevant ideal. We will show that the following polynomials give a Groebner basis for $S^G \cap \mathfrak{m}^{[p^m]}$.

Definition 4.3. *Define polynomials in $S^G = \mathbb{F}_p[f_1, \ldots, f_n]$ for $1 \le a \le b < n$ by*

$$h_0 = f_n^{1+e^{-1}(p^m-1)}, \quad h_{1,a} = \sum_{k=0}^{m-1} f_n^{1+e^{-1}(p^m-p^{m-k})}\, f_a^{p^{m-k-1}}, \text{ and } h_{2,a,b} = f_a^{p^{m-1}} f_b^{p^{m-1}}.$$

Example 4.4. For our archetype example $G = \left\langle \begin{pmatrix} 1&0&0\\0&1&0\\0&0&\omega \end{pmatrix}, \begin{pmatrix} 1&0&1\\0&1&0\\0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0\\0&1&1\\0&0&1 \end{pmatrix} \right\rangle \subset \mathrm{GL}_3(\mathbb{F}_5)$,

$$h_0 = f_3^{1+e^{-1}(5^m-1)},$$

$$h_{1,1} = \sum_{k=0}^{m-1} f_3^{1+e^{-1}(5^m-5^{m-k})}\, f_1^{5^{m-k-1}}, \quad h_{1,2} = \sum_{k=0}^{m-1} f_3^{1+e^{-1}(5^m-5^{m-k})}\, f_2^{5^{m-k-1}},$$

$$h_{2,1,1} = f_1^{2(5^{m-1})}, \quad h_{2,1,2} = f_1^{5^{m-1}} f_2^{5^{m-1}}, \quad \text{and } h_{2,2,2} = f_2^{2(5^{m-1})}.$$

The next lemma verifies that these polynomials lie in the Frobenius irrelevant ideal.

Lemma 4.5. *For G with maximal transvection root space, the polynomials h_0, $h_{1,a}$, $h_{2,a,b}$ for $1 \le a \le b < n$ lie in $S^G \cap \mathfrak{m}^{[p^m]}$.*

Proof. Straight-forward computation confirms that

$$h_0 = x_n^{p^m+e-1}, \quad h_{1,a} = x_a^{p^m} x_n^e - x_a x_n^{p^m+e-1}, \quad \text{and}$$

$$h_{2,a,b} = x_a^{p^m} x_b^{p^m} - x_a^{p^{m-1}} x_b^{p^m} x_n^{(p-1)p^{m-1}} - x_a^{p^m} x_b^{p^{m-1}} x_n^{(p-1)p^{m-1}} + x_a^{p^{m-1}} x_b^{p^{m-1}} x_n^{2(p-1)p^{m-1}}.$$

□

The next key lemma describes elements of $S^G \cap \mathfrak{m}^{[p^m]}$; it relies on an inductive argument using Lucas' Theorem on binomial coefficients (see [10] or [12, Exercise 1.6(a)]).

Lemma 4.6. *If G has maximal transvection root space and $f \in S^G \cap \mathfrak{m}^{[p^m]}$ is homogeneous in $f_1, \ldots, f_n$, then $\mathrm{LM}_{S^G}(f)$ is divisible by f_n or some $h_{2,a,b}$ with $1 \le a \le b < n$.*

Proof. Suppose no $h_{2,a,b}$ divides $\mathrm{LM}_{S^G}(f)$ nor f_n. Then

$$\mathrm{LM}_{S^G}(f) = f_1^{c_1} f_2^{c_2} \cdots f_{n-1}^{c_{n-1}}$$

for some $c_i < 2p^{m-1}$ (as no $h_{2,a,a}$ divides) with all but possibly one exponent satisfying $c_i < p^{m-1}$ (as no $h_{2,a,b}$ divides for $a \neq b$). Observe first that not all $c_i < p^{m-1}$. Otherwise, by the binomial theorem and Eq. (4.1),

$$\mathrm{LM}_S(f) = \mathrm{LM}_S(\mathrm{LM}_{S^G}(f)) = x_1^{c_1 p} x_2^{c_2 p} \cdots x_{n-1}^{c_{n-1} p}$$

would not lie in the monomial ideal $\mathfrak{m}^{[p^m]}$, contradicting the fact that f does. Hence there is a unique index j with $p^{m-1} \le c_j < 2p^{m-1}$. Without loss of generality, say $j = 1$, so that $p^{m-1} \le c_1 < 2p^{m-1}$ and $c_i < p^{m-1}$ for $1 < i < n$. Define h by

$$h = f \cdot f_1^{2p^{m-1}-c_1-1} f_2^{p^{m-1}-c_2-1} f_3^{p^{m-1}-c_3-1} \cdots f_{n-1}^{p^{m-1}-c_{n-1}-1}.$$

We will produce a monomial

$$x_\alpha = x_1^{p^m-p+1} x_2^{p^m-p} x_3^{p^m-p} \cdots x_{n-1}^{p^m-p} x_n^{p^m-1}$$

of h in the variables $x_1, \ldots, x_n$ which does not lie in $\mathfrak{m}^{[p^m]}$. This will imply that h itself does not lie in $\mathfrak{m}^{[p^m]}$, contradicting the fact that h is a multiple of f.

To this end, set $L = \mathrm{LM}_{S^G}(h)$, so that, by construction,

$$L = \mathrm{LM}_{S^G}(h) = f_1^{2p^{m-1}-1} f_2^{p^{m-1}-1} \cdots f_{n-1}^{p^{m-1}-1}.$$

We write L as a polynomial in the variables $x_1, \ldots, x_n$ using the binomial theorem. Direct calculation in $S/\mathfrak{m}^{[p^m]}$ confirms that

$$L + \mathfrak{m}^{[p^m]} = \pm\, x_\alpha + \mathfrak{m}^{[p^m]}$$

as Lucas' Theorem implies that

$$\binom{2p^{m-1}-1}{\sum_{i=0}^{m-1} p^i} = \begin{cases} 1 & \text{for } m = 1, 2, \\ \prod_{i=0}^{m-2} \binom{p-1}{1} = (-1)^{m-1} & \text{for } m > 2\,. \end{cases}$$

Thus, the monomial x_α appears with nonzero coefficient in L and does not lie in $\mathfrak{m}^{[p^m]}$.

We now argue that x_α appears with nonzero coefficient in h itself (i.e., does not cancel with other terms). Consider the coefficient $c_\alpha(M)$ of x_α in some other monomial

$$M = f_1^{c_1'} f_2^{c_2'} \cdots f_n^{c_n'} \quad < \quad L$$

of h after expanding M in the variables $x_1, \ldots, x_n$ and suppose $c_\alpha(M) \neq 0$.

We first establish that M has smaller degree in f_1 than L but larger degree in f_n. Indeed, note that $p^{m-1} \le c_1'$, else $\deg_{x_1}(M) < \deg_{x_1}(x_\alpha)$ and $c_\alpha(M) = 0$. Now fix $1 < i < n$ and consider c_i'. Note that $c_i' \ge p^{m-1} - 1$ else $c_\alpha(M) = 0$ as $f_k \in \mathbb{F}_p[x_k, x_n]$ for all k. And $c_i' \le p^{m-1} - 1$ else $h_{2,1,i}$ divides M and $c_\alpha(M) = 0$ as $M \in \mathfrak{m}^{[p^m]}$. Thus

$c'_i = p^{m-1} - 1$ and $\deg_{f_i}(M) = \deg_{f_i}(L)$ for $1 < i < n$. But $\deg_S M = \deg_S L$, with $M < L$. Thus M has smaller degree in f_1 but larger degree in f_n than L, i.e.,

- $p^{m-1} \le c'_1 < 2p^{m-1} - 1$, and
- $c'_i = p^{m-1} - 1$ for $1 < i < n$, and
- $c'_n > 0$.

We assume $m \ge 2$ since if $m = 1$, then $c'_1 = 0$ and $\deg_{x_1}(M) = 0$, forcing $c_\alpha(M) = 0$.

We examine the contribution to M from f_1. Set $d = c'_1$. Then as $c_\alpha \ne 0$ and

$$f_1^d = (x_1^p - x_1 x_n^{p-1})^d = \sum_{i=0}^{d} \binom{d}{i} \, x_1^{dp-(p-1)i} x_n^{(p-1)i} \, ,$$

there is some index i with $\binom{d}{i} \ne 0$ and $dp - (p-1)i = p^m - p + 1$. Hence $i \equiv 1 \mod p$. Since $d < 2p^{m-1} - 1$ by assumption,

$$d = p^{m-1} + (p-1)a \quad \text{and} \quad i = 1 + pa \quad \text{for some} \quad 0 \le a < \sum_{k=0}^{m-2} p^k \, . \tag{4.7}$$

We show instead that $\sum_{k=0}^{m-2} p^k \le a$ by considering the base p expansions of a and d:

$$a = \sum_{k=0}^{m-2} a_k \, p^k \quad \text{and} \quad d = \sum_{k=0}^{m-1} d_k \, p^k \quad \text{for some} \quad 0 \le a_k, \, d_k < p.$$

We compare the base p coefficients d_k and a_k using the key point that $\binom{d}{i}$ is nonzero: Lucas' Theorem implies that

$$0 \ne \binom{d}{i} = \binom{d_0}{1} \prod_{k=1}^{m-1} \binom{d_k}{a_{k-1}} \quad \text{as } i = 1 + \sum_{k=1}^{m-1} a_{k-1} \, p^k \, ;$$

since no factor in the product vanishes, we conclude that $d_0 \ge 1$ and each $a_{k-1} \le d_k$. Eq. (4.7) then provides direct comparison of d_k and a_k,

$$\sum_{k=0}^{m-1} d_k \, p^k \; = \; d \; = \; p^{m-1} - a_0 + \sum_{k=1}^{m-2} (a_{k-1} - a_k) p^{k+1} + a_{m-2} p^{m-1}. \tag{4.8}$$

We now regroup base p as needed and show inductively that $0 < a_0 \le a_1 \le \ldots \le a_{m-2}$.

We first consider a_0. Since $1 \le d_0$, Eq. (4.8) implies that $d_0 = p - a_0$ and $a_0 \ne 0$. For $m > 2$, next observe that $a_0 \le a_1$ since $a_0 \le d_1$ and Eq. (4.8) implies that

$$d_1 = p + a_0 - a_1 - 1 \text{ for } a_0 \le a_1 \quad \text{whereas} \quad d_1 = a_0 - a_1 - 1 \text{ for } a_1 < a_0.$$

Similarly, $a_1 \le a_2$ since $a_1 \le d_2$ and Eq. (4.8) implies that

$$d_2 = p + a_1 - a_2 - 1 \text{ for } a_1 \le a_2 \quad \text{whereas} \quad d_2 = a_1 - a_2 - 1 \text{ for } a_2 < a_1.$$

We iterate this argument and conclude that $0 < a_0 \le a_1 \le \ldots \le a_{m-2}$. But this contradicts Eq. (4.7), so $\binom{d}{i} = 0$ and thus $c_\alpha(M) = 0$. □

We now show that the collection of h_0, $h_{1,a}$, $h_{2,a,b}$ is a Groebner basis.

Proposition 4.9. *If G has maximal transvection root space, then the ideal $S^G \cap \mathfrak{m}^{[p^m]}$ of S^G has as a Groebner basis $\mathscr{G} = \{h_0, \, h_{1,a}, \, h_{2,a,b} : \, 1 \le a \le b < n\}$.*

Proof. Suppose f in $S^G \cap \mathfrak{m}^{[p^m]}$ is homogeneous in the variables $f_1, \ldots, f_n$. Say neither $h_0 = \mathrm{LM}_{S^G}(h_0)$ nor any $h_{2,a,b} = \mathrm{LM}_{S^G}(h_{2,a,b})$ for $1 \le a \le b < n$ divide $\mathrm{LM}_{S^G}(f)$. We show $\mathrm{LM}_{S^G}(h_{1,j})$ divides $\mathrm{LM}_{S^G}(f)$ for some $1 \le j < n$. We write

$$\mathrm{LM}_{S^G}(f) = f_1^{c_1} f_2^{c_2} \cdots f_n^{c_n}$$

for some $c_n < \deg_{f_n}(h_0) = 1 + (p^m - 1)/e$ and some $c_1, \ldots, c_{n-1}$. But f and hence $\mathrm{LM}_S(f)$ lies in $\mathfrak{m}^{[p^m]}$, so $p^{m-1} \le c_j$ for some index $j < n$ since

$$\mathrm{LM}_S(f) = \mathrm{LM}_S\left(\mathrm{LM}_{S^G}(f)\right) = x_1^{pc_1} x_2^{pc_2} \ldots x_{n-1}^{pc_{n-1}} x_n^{ec_n} .$$

Then $f_j^{p^{m-1}}$ divides $\mathrm{LM}_{S^G}(f)$. Lemma 4.6 implies that $\mathrm{LM}_{S^G}(f)$ is also divisible by f_n, hence by $\mathrm{LM}_{S^G}(h_{1,j}) = f_j^{p^{m-1}} f_n$ as well. As $\mathscr{G} \subset S^G \cap \mathfrak{m}^{[p^m]}$ by Lemma 4.5, $\mathscr{G}$ is a Groebner basis for $S^G \cap \mathfrak{m}^{[p^m]}$.

$\square$

Example 4.10. For $G = \left\langle \left(\begin{smallmatrix} 1&0&0\\0&1&0\\0&0&\omega \end{smallmatrix}\right), \left(\begin{smallmatrix} 1&0&1\\0&1&0\\0&0&1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1&0&0\\0&1&1\\0&0&1 \end{smallmatrix}\right) \right\rangle \subset \mathrm{GL}_3(\mathbb{F}_5)$, the polynomials

$$h_0 = f_3^{1+e^{-1}(5^m-1)}, \quad h_{1,1} = \sum_{k=0}^{m-1} f_3^{1+e^{-1}(5^m-5^{m-k})}\ f_1^{5^{m-k-1}}, \quad h_{2,2,2} = f_2^{2(5^{m-1})},$$

$$h_{1,2} = \sum_{k=0}^{m-1} f_3^{1+e^{-1}(5^m-5^{m-k})}\ f_2^{5^{m-k-1}}, \quad h_{2,1,1} = f_1^{2(5^{m-1})}, \quad \text{and} \quad h_{2,1,2} = f_1^{5^{m-1}} f_2^{5^{m-1}}$$

form a Groebner basis for $S^G \cap \mathfrak{m}^{[5^m]}$ as an ideal of S^G.

5. Hilbert Series of invariants in the Frobenius Irrelevant Ideal

Again, we assume G is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ fixing a hyperplane H and set e to be the maximal order of a semisimple element of G. We consider the case when G has maximal transvection root space, i.e., the case when G is generated by $n-1$ transvections together possibly with a semisimple reflection of order e. For any graded module M, we write $M[i]$ for the graded module with degrees shifted down by i so that $M[i]_d = M_{i+d}$.

Proposition 5.1. *Suppose G has maximal transvection root space. Then*

$$\mathrm{Hilb}\left(S^G + \mathfrak{m}^{[p^m]} \big/ \mathfrak{m}^{[p^m]},\ t\right) = \left(\frac{1-t^{p^m}}{1-t^p}\right)^{n-1} \left(\frac{1 - t^{p^m+e-1} + (n-1)\, t^{p^m}(1-t^e)}{1-t^e}\right).$$

Proof. We replace the ideal $S^G \cap \mathfrak{m}^{[p^m]}$ by its initial ideal with respect to the graded lexicographical order on $\mathbb{F}_p[x_1, \ldots, x_n]$ with $x_1 > \cdots > x_n$, since (see, for example, [4])

$$\mathrm{Hilb}\left(S^G + \mathfrak{m}^{[p^m]} \big/ \mathfrak{m}^{[p^m]},\ t\right) = \mathrm{Hilb}\left(S^G \big/ (S^G \cap \mathfrak{m}^{[p^m]}),\ t\right) = \mathrm{Hilb}\left(S^G \big/ \mathrm{in}(S^G \cap \mathfrak{m}^{[p^m]}),\ t\right).$$

We compute the Hilbert series recursively using short exact sequences. By Proposition 4.9, $\mathscr{G}$ is a Groebner basis for $S^G \cap \mathfrak{m}^{[p^m]}$, and we enumerate the various elements h_0, $h_{1,a}$, and $h_{2,a,b}$ in $\mathscr{G}$ as $h_1, h_2, h_3, \ldots, h_{n-1+\binom{n}{2}}$ by setting

$$h_k = h_{1,k} \quad \text{for } 1 \le k < n \quad \text{and} \quad h_{na+b-\binom{a+1}{2}} = h_{2,a,b} \quad \text{for } 1 \le a \le b < n\,.$$

Set $M_{n+\binom{n}{2}} = 1$ (for ease with notation), $I_0 = \big(M_0\big)$, $M_i = \mathrm{LM}_{S^G}(h_i)$ and

$$J_i = \big(M_j/\gcd(M_j, M_{i+1}) : 0 \le j \le i\big) \quad \text{for } 0 \le i \le n-1+\tbinom{n}{2}.$$

Note that $I_{n-1+\binom{n}{2}} = \mathrm{in}(S^G \cap \mathfrak{m}^{[p^m]})$. This gives the short exact sequence (for each i)

$$0 \longrightarrow \big(S^G\!\diagup J_i\big)\big[-\deg(M_{i+1})\big] \longrightarrow S^G\!\diagup I_i \longrightarrow S^G\!\diagup I_{i+1} \longrightarrow 0\,. \tag{5.2}$$

Each ideal I_i is uniquely determined by some polynomial h_i of the form h_0, $h_{1,a}$, or $h_{2,a,b}$, and we revert to more suggestive notation for the next computations, defining

$$I^0 = I_0, \qquad I^{1,k} = I_k,\ \ I^{2,a,b} = I_{na+b-\binom{a+1}{2}} \quad \text{for } 1 \le k < n,\ 1 \le a \le b < n\,;$$
$$J^0 = J_0, \qquad J^{1,k} = J_k,\ \ J^{2,a,b} = J_{na+b-\binom{a+1}{2}} \quad \text{for } 1 \le k < n,\ 1 \le a \le b < n\,,$$

so that the ideals $I_1, I_2, \ldots, I_{n-1+\binom{n}{2}}$ merely enumerate the ideals $I^0, I^{1,a}, I^{2,a,b}$ for ease with induction, with the last ideal in our sequence just

$$I^{2,n-1,n-1} = I_{n-1+\binom{n}{2}} = \mathrm{in}(S^G \cap \mathfrak{m}^{[p^m]})\,.$$

To find the Hilbert series for S^G/J_i, we first give minimal generating sets for each J_i,

$$\begin{aligned}
J^0 &= \big(f_n^{e^{-1}(p^m-1)}\big),\\
J^{1,a} &= \big(f_n^{e^{-1}(p^m-1)}, f_j^{p^{m-1}} : 1 \le j \le a\big) && \text{for } \ 1 \le a \le n-2,\\
J^{1,n-1} &= (f_n),\\
J^{2,a,b} &= \big(f_n, f_j^{p^{m-1}} : 1 \le j \le b\big) && \text{for } \ 1 \le a \le b \le n-2,\\
J^{2,a,n-1} &= \big(f_n, f_j^{p^{m-1}} : 1 \le j \le a\big) && \text{for } \ 1 \le a \le n-2\,,
\end{aligned}$$

and then use the additivity of Hilbert series over short exact sequences of the form

$$0 \longrightarrow (f_n^d) \longrightarrow S^G \longrightarrow S^G\!\diagup (f_n^d) \longrightarrow 0 \qquad \text{and}$$
$$0 \longrightarrow S^G\!\diagup\big(f_n^d, f_i^{p^{m-1}} : 1 \le i < c\big)[-p^m] \longrightarrow S^G\!\diagup\big(f_n^d, f_i^{p^{m-1}} : 1 \le i < c\big) \longrightarrow S^G\!\diagup\big(f_n^d, f_i^{p^{m-1}} : 1 \le i \le c\big) \longrightarrow 0$$

(for $d = 1$ or $d = e^{-1}(p^m - 1)$ and $1 \le c \le n-1$). We conclude that

(5.3)

$$\begin{aligned}
\mathrm{Hilb}\big(S^G\!\diagup J^0,\ t\big) &= \frac{1 - t^{p^m-1}}{(1-t^e)(1-t^p)^{n-1}}\,,\\
\mathrm{Hilb}\big(S^G\!\diagup J^{1,a},\ t\big) &= \frac{(1-t^{p^m})^a(1-t^{p^m-1})}{(1-t^e)(1-t^p)^{n-1}} && \text{for } \ 1 \le a \le n-2\,,\\
\mathrm{Hilb}\big(S^G\!\diagup J^{1,n-1},\ t\big) &= \frac{1-t^e}{(1-t^e)(1-t^p)^{n-1}}\,,\\
\mathrm{Hilb}\big(S^G\!\diagup J^{2,a,b},\ t\big) &= \frac{(1-t^{p^m})^b(1-t^e)}{(1-t^e)(1-t^p)^{n-1}} && \text{for } \ 1 \le a \le b \le n-2 \quad \text{and,}\\
\mathrm{Hilb}\big(S^G\!\diagup J^{2,a,n-1},\ t\big) &= \frac{(1-t^{p^m})^a(1-t^e)}{(1-t^e)(1-t^p)^{n-1}} && \text{for } \ 1 \le a \le n-2\,.
\end{aligned}$$

Then as

$$\mathrm{Hilb}\left(S^G\!\big/I^0,\ t\right) = \frac{1-t^{p^m+e-1}}{(1-t^e)(1-t^p)^{n-1}}\,, \tag{5.4}$$

Equations (5.2) to (5.4) imply that $\mathrm{Hilb}\left(S^G/\mathrm{in}(S^G\cap\mathfrak{m}^{[p^m]})\,,\,t\right)$ is

$$\underbrace{\frac{1-t^{p^m+e-1}}{(1-t^e)(1-t^p)^{n-1}}}_{I^0} \underbrace{-\,t^{p^m+e}\frac{1-t^{p^m-1}}{(1-t^e)(1-t^p)^{n-1}}}_{J^0} \underbrace{-\,t^{p^m+e}\sum_{a=1}^{n-2}\frac{(1-t^{p^m})^a(1-t^{p^m-1})}{(1-t^e)(1-t^p)^{n-1}}}_{J^{1,a}}$$

$$\underbrace{-\,t^{2p^m}\frac{1-t^e}{(1-t^e)(1-t^p)^{n-1}}}_{J^{1,n-1}} \underbrace{-\,t^{2p^m}\sum_{b=1}^{n-2}\sum_{a=1}^{b}\frac{(1-t^{p^m})^b(1-t^e)}{(1-t^e)(1-t^p)^{n-1}}}_{J^{2,a,b}} \underbrace{-\,t^{2p^m}\sum_{a=1}^{n-2}\frac{(1-t^{p^m})^a(1-t^e)}{(1-t^e)(1-t^p)^{n-1}}}_{J^{2,a,n-1}}\ .$$

We combine summations to express $\mathrm{Hilb}\left(S^G/\mathrm{in}(S^G\cap\mathfrak{m}^{[p^m]})\,,\,t\right)$ as

$$\begin{aligned}&\frac{1-t^{p^m+e-1}}{(1-t^e)(1-t^p)^{n-1}} - t^{p^m+e}\sum_{a=0}^{n-2}\frac{(1-t^{p^m})^a(1-t^{p^m-1})}{(1-t^e)(1-t^p)^{n-1}}\\ &\qquad - t^{2p^m}(1-t^e)\sum_{b=1}^{n-2}\sum_{a=1}^{b}\frac{(1-t^{p^m})^b}{(1-t^e)(1-t^p)^{n-1}} - t^{2p^m}\sum_{a=0}^{n-2}\frac{(1-t^{p^m})^a(1-t^e)}{(1-t^e)(1-t^p)^{n-1}}\,,\end{aligned}$$

which simplifies (using elementary series formulas) to

$$\begin{aligned}&\frac{1-t^{p^m+e-1}}{(1-t^e)(1-t^p)^{n-1}} - t^{p^m+e}\frac{\big(1-(1-t^{p^m})^{n-1}\big)(1-t^{p^m-1})}{t^{p^m}(1-t^e)(1-t^p)^{n-1}}\\ &\qquad - t^{2p^m}(1-t^e)\sum_{b=1}^{n-2}\frac{b(1-t^{p^m})^b}{(1-t^e)(1-t^p)^{n-1}} - t^{2p^m}\frac{\big(1-(1-t^{p^m})^{n-1}\big)(1-t^e)}{t^{p^m}(1-t^e)(1-t^p)^{n-1}}\ .\end{aligned}$$

We use the fact that

$$\sum_{b=1}^{n-2} b\,(1-t^{p^m})^b \;=\; \frac{-(1-t^{p^m})\big((n-1)(1-t^{p^m})^{n-2}\ t^{p^m}+1-(1-t^{p^m})^{n-1}\big)}{t^{2p^m}}$$

to rewrite this last expression as

$$\mathrm{Hilb}\left(S^G\!\big/\mathrm{in}(S^G\cap\mathfrak{m}^{[p^m]})\,,\ t\right) \;=\; \frac{(1-t^{p^m})^{n-1}\big(1-t^{p^m+e-1}+(n-1)t^{p^m}(1-t^e)\big)}{(1-t^e)(1-t^p)^{n-1}}\ .$$

□

Example 5.5. For $G=\left\langle \left(\begin{smallmatrix}1&0&0\\0&1&0\\0&0&\omega\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0&1\\0&1&0\\0&0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0&0\\0&1&1\\0&0&1\end{smallmatrix}\right)\right\rangle \subset \mathrm{GL}_3(\mathbb{F}_5)$, Proposition 5.1 gives

$$\mathrm{Hilb}\left((S^G+\mathfrak{m}^{[5^m]})\big/\mathfrak{m}^{[5^m]},\ t\right) \;=\; \frac{(1-t^{5^m})^2\big(1-t^{5^m+e-1}+2t^{5^m}(1-t^e)\big)}{(1-t^e)(1-t^5)^2}\ .$$

6. Decomposition of the invariant space

We now use the description of $S^G \cap \mathfrak{m}^{[p^m]}$ from the last two sections to give a direct sum decomposition of $(S/\mathfrak{m}^{[p^m]})^G$. Again, we consider a subgroup G of $\mathrm{GL}_n(\mathbb{F}_p)$ fixing a hyperplane and use the basis $x_1, \dots, x_n$ of V^* and basic invariants $f_1, \dots, f_n$ as in Section 3. We show that $(S/\mathfrak{m}^{[p^m]})^G$ is the direct sum of subspaces

$$A_G = {(S^G + \mathfrak{m}^{[p^m]})}\big/{\mathfrak{m}^{[p^m]}} \quad \text{and}$$

$$B_G = \mathbb{F}_p[f_1, \dots, f_{n-1}]\text{-span}\Big\{x_1^{a_1} \dots x_\ell^{a_\ell} x_n^{p^m-1} + \mathfrak{m}^{[p^m]} : 0 \le a_i < p, \sum_{i=1}^{\ell} a_i \ge 2\Big\}.$$

Note that B_G is the $\mathbb{F}_p[f_1, \dots, f_{n-1}]$-submodule of $S/\mathfrak{m}^{[p^m]}$ spanned by the monomial cosets indicated. Recall that ℓ is the minimal number of transvections generating G together with a semisimple element of order e; if no group elements are semisimple, $e = 1$.

Remark 6.1. In defining the subspace B_G, we require $\sum_{i=1}^{\ell} a_i \ge 2$ to avoid nontrivial intersection with A_G; see Proposition 6.5. Otherwise B_G would contain $x_n^{p^m-1} + \mathfrak{m}^{[p^m]}$ and $x_i x_n^{p^m-1} + \mathfrak{m}^{[p^m]}$, for example, which lie in A_G for $i < \ell$.

We first describe the leading monomial in $(S/\mathfrak{m}^{[p^m]})^G$ using the standard graded lexicographical order on $S = \mathbb{F}_p[x_1, \dots, x_n]$ with $x_1 > \dots > x_n$.

Lemma 6.2. *Assume G has maximal transvection root space. Suppose $f + \mathfrak{m}^{[p^m]}$ lies in $(S/\mathfrak{m}^{[p^m]})^G$ with f homogeneous in $x_1, \dots, x_n$. Then $\mathrm{LM}_S(f)$ lies in*

$$\mathfrak{m}^{[p^m]} \qquad or \qquad \mathbb{F}_p[x_1, \dots, x_{n-1}, f_n^{e^{-1}(p^m-1)}] \qquad or \qquad \mathbb{F}_p[x_1^p, \dots, x_{n-1}^p, f_n]\,.$$

Proof. Say $M = \mathrm{LM}_S(f)$ does not lie in $\mathfrak{m}^{[p^m]}$ or in $\mathbb{F}_p[x_1, \dots, x_{n-1}, f_n^{e^{-1}(p^m-1)}]$. Then

$$M = x_1^{b_1} \cdots x_k^{b_k} \cdots x_{n-1}^{b_{n-1}} x_n^{b_n} \qquad \text{for some } \ b_1, \dots, b_{n-1} < p^m \text{ and } b_n < p^m - 1\,.$$

We use the generators $g_1, \dots, g_n$ of G from Section 3. Since f is G-invariant modulo $\mathfrak{m}^{[p^m]}$, the difference $g_n f - f$ lies in $\mathfrak{m}^{[p^m]}$ and the low degree of each x_i forces f itself to be invariant under g_n; hence b_n is divisible by e.

Suppose there is some exponent b_k which is not divisible by p with $k < n$. Consider $g = g_k^{-1}$ acting on $M = \mathrm{LM}_S(f)$. Then $g \cdot M - M$ is

$$x_1^{b_1} \cdots x_{k-1}^{b_{k-1}} \big((x_k + x_n)^{b_k} - x_k^{b_k}\big)\, x_{k+1}^{b_{k+1}} \cdots x_n^{b_n}$$

with leading monomial

$$\mathrm{LM}_S(gM - M) = x_1^{b_1} \cdots x_{k-1}^{b_{k-1}} \,(b_k\, x_k^{b_k - 1})\, x_{k+1}^{b_{k+1}} x_{k+2}^{b_{k+2}} \cdots x_{n-1}^{b_{n-1}} x_n^{b_n+1} \tag{6.3}$$

as $b_k \neq 0$ in $\mathbb{F}_p$. Notice that the leading monomial of $gM - M$ is the leading monomial of $gf - f$ as M is the leading monomial of f and g fixes $x_1, \dots, x_{k-1}, x_{k+1}, \dots, x_n$.

Since f is invariant modulo $\mathfrak{m}^{[p^m]}$, the difference $gf - f$ and thus its leading monomial (6.3) lie in $\mathfrak{m}^{[p^m]}$. But this is impossible as $b_n < p^m - 1$ and $b_1, \dots, b_{n-1} < p^m$ by our assumptions. Thus p must divide every exponent b_k for $k < n$. $\square$

We use Lemma 6.2 to decompose the invariants of the quotient space.

Proposition 6.4. *For G with maximal transvection root space, $\left({S}/{\mathfrak{m}^{[p^m]}}\right)^G = A_G + B_G$.*

Proof. By construction, $A_G \subseteq (S/\mathfrak{m}^{[p^m]})^G$. To show $B_G \subseteq (S/\mathfrak{m}^{[p^m]})^G$, consider

$$M = x_1^{a_1} \dots x_{n-1}^{a_{n-1}} x_n^{p^m-1} \quad \text{ with } M + \mathfrak{m}^{[p^m]} \in B_G.$$

We consider the generators $g_1, \dots, g_n$ of G from Section 3; for $k < n$,

$$\begin{aligned} g_k^{-1}(M) + \mathfrak{m}^{[p^m]} &= x_1^{a_1} \dots x_{k-1}^{a_{k-1}} (x_k + x_n)^{a_k} x_{k+1}^{a_{k+1}} \dots x_{n-1}^{a_{n-1}} x_n^{p^m-1} + \mathfrak{m}^{[p^m]} \\ &= x_1^{a_1} \dots x_{n-1}^{a_{n-1}} x_n^{p^m-1} + \mathfrak{m}^{[p^m]} \;=\; M + \mathfrak{m}^{[p^m]}, \end{aligned}$$

since the binomial theorem implies that all but the initial term lies in $\mathfrak{m}^{[p^m]}$. In addition, e divides p^m-1, so g_n fixes M. Hence B_G is G-invariant and thus $A_G + B_G \subseteq (S/\mathfrak{m}^{[p^m]})^G$.

To show the reverse containment, we first argue that any monomial M in the variables $x_1, \dots, x_n$ with $\deg_{x_n}(M) = p^m - 1$ represents a coset of $\mathfrak{m}^{[p^m]}$ either in A_G or in B_G. Both A_G and B_G are closed under multiplication by $f_1, \dots, f_{n-1}$, so we assume without loss of generality that $\deg_{x_i}(M) < p$ for $i < n$ by Eq. (4.2). Let $k = \sum_{i=1}^{n-1} \deg_{x_i}(M)$. If $k \geq 2$, then $M + \mathfrak{m}^{[p^m]}$ lies in B_G by definition. If $k = 0$, then $M = x_n^{p^m-1} = f_n^{e^{-1}(p^m-1)}$ and $M + \mathfrak{m}^{[p^m]}$ lies in A_G. If $k = 1$, then $M + \mathfrak{m}^{[p^m]}$ lies in A_G as well since

$$-x_i\, x_n^{p^m-1} \equiv \sum_{j=0}^{m-1} f_n^{e^{-1}(p^m-p^j)} f_i^{p^{m-1-j}} \quad \bmod \mathfrak{m}^{[p^m]} \quad \text{for } i < n.$$

If the reverse containment fails, we may choose some $f + \mathfrak{m}^{[p^m]}$ in $(S/\mathfrak{m}^{[p^m]})^G$ but not in $A_G + B_G$ with f homogeneous in $x_1, \dots, x_n$ and $\mathrm{LM}_S(f)$ minimal. Note that $\deg_{x_i}(\mathrm{LM}_S(f)) < p^m$ for all i. By the minimality assumption, $\mathrm{LM}_S(f) + \mathfrak{m}^{[p^m]}$ does not lie in A_G or B_G, so by the argument in the last paragraph, $\deg_{x_n}(\mathrm{LM}_S(f)) < p^m - 1$. By Lemma 6.2, the monomial $\mathrm{LM}_S(f)$ lies in $\mathbb{F}_p[x_1^p, \dots, x_{n-1}^p, f_n]$, so

$$\mathrm{LM}_S(f) = x_1^{pc_1} x_2^{pc_2} \cdots x_{n-1}^{pc_2}\, x_n^{ec_n} \quad \text{ for some } c_i\,.$$

Define h by

$$h = \alpha f_1^{c_1} f_2^{c_2} \cdots f_{n-1}^{c_{n-1}}\, f_n^{c_n}, \quad \text{for } \alpha \text{ the leading coefficient of } f.$$

Then $f - h + \mathfrak{m}^{[p^m]}$ lies in $(S/\mathfrak{m}^{[p^m]})^G$ since $h + \mathfrak{m}^{[p^m]}$ lies in A_G, and, by construction, $\mathrm{LM}_S(h) = \mathrm{LM}_S(f)$, implying that $\mathrm{LM}_S(f-h) < \mathrm{LM}_S(f)$. The minimality assumption then implies that $f - h$ must lie in $A_G + B_G$. However, $A_G + B_G$ contains h already, so must contain f as well, contradicting our choice of f. Thus $(S/\mathfrak{m}^{[p^m]})^G = A_G + B_G$. $\square$

Proposition 6.5. *Suppose the transvection root space of G is maximal. Then*

$$\left({S}/{\mathfrak{m}^{[p^m]}}\right)^G = A_G \oplus B_G\,.$$

Proof. By Proposition 6.4, we need only show $A_G \cap B_G$ is trivial. If $m \leq 1$, a simple degree comparison shows $A_G \cap B_G = \{0\}$, hence we assume $m \geq 2$. Suppose $A_G \cap B_G$ is non-trivial, say some f in S^G and $h + \mathfrak{m}^{[p^m]}$ in B_G satisfy

$$0 \neq f + \mathfrak{m}^{[p^m]} = h + \mathfrak{m}^{[p^m]} \in A_G \cap B_G\,.$$

We multiply $f-h$ by $f_n = x_n^e$ so that $(f-h)f_n$ lies in $\mathfrak{m}^{[p^m]} f_n$. We will show that ff_n and hf_n have no monomials in the variables $x_1, \ldots, x_n$ in common; this will force hf_n to lie in $\mathfrak{m}^{[p^m]} f_n$, contradicting the fact that h does not lie in $\mathfrak{m}^{[p^m]}$.

Fix some M in $X_f \cap X_h$ for

$$X_f \text{ the set of monomials in } x_1, \ldots, x_n \text{ of } ff_n, \text{ and}$$
$$X_h \text{ the set of monomials in } x_1, \ldots, x_n \text{ of } hf_n\,.$$

Since h lies in the ideal $(x_n^{p^m-1})$ and $e \geq 1$, the ideal $\mathfrak{m}^{[p^m]}$ contains hf_n and thus also $ff_n = (f-h)f_n + hf_n$. However, ff_n also lies in S^G, so ff_n lies in $S^G \cap \mathfrak{m}^{[p^m]}$. Proposition 4.9 then implies that M is a monomial of some S^G-multiple of h_0, $h_{1,a}$, or $h_{2,a,b}$ for some $1 \leq a \leq b < n$ (see Definition 4.3) and we use Lemma 4.5 to expand in the variables $x_1, \ldots, x_n$. Since h is not in $\mathfrak{m}^{[p^m]}$ and M lies in X_h, Eq. (4.2) implies that

$$\deg_{x_n}(M) = p^m + e - 1 \quad \text{and} \tag{6.6}$$

$$\deg_{x_i}(M) = b_i\, p + a_i \text{ for some } b_i < p^{m-1}, a_i < p, \text{ with } \textstyle\sum_{i=1}^{n-1} a_i \geq 2\,. \tag{6.7}$$

First, say M is a monomial of some polynomial in $S^G\, h_0$. By Lemma 4.5, for $i < n$,

$$\deg_{x_n}(M) = x_n^{p^m+e-1+c_n+(p-1)\sum_{i=1}^{n-1} j_i} \qquad \text{and}$$
$$\deg_{x_i}(M) = pc_i - (p-1)j_i = (c_i - j_i)p + j_i \qquad \text{for some } c_i \in \mathbb{N} \text{ and } 0 \leq j_i \leq c_i\,.$$

But Eq. (6.6) implies that $j_i = 0$ for all $i < n$ and $c_n = 0$. Then p must divide $\deg_{x_i}(M)$ for each $1 \leq i \leq n$, contradicting Eq. (6.7).

Second, say that M is a monomial of some polynomial in $S^G\, h_{1,a}$ for some $a < n$. Without loss of generality, say $a = 1$. Then, for $1 < i < n$,

$$\deg_{x_i}(M) = pc_i - (p-1)j_i \qquad \text{for some } \ c_i \in \mathbb{N} \ \text{ and } 0 \leq j_i \leq c_i\,.$$

Furthermore, by Lemma 4.5,

$$\deg_{x_1}(M) = p^m + pc_1 - (p-1)j_1 \qquad \text{or} \qquad \deg_{x_1}(M) = 1 + pc_1 - (p-1)j_1$$

for some $c_1 \in \mathbb{N}$ and $1 \leq j_1 \leq c_1$. But Eq. (6.7) implies the latter case holds, and thus

$$\deg_{x_n}(M) = p^m + e - 1 + c_n + (p-1)\textstyle\sum_{i=1}^{n-1} j_i \qquad \text{for some } c_n \in \mathbb{N}\,.$$

Again, Eq. (6.6) implies $j_i = 0$ for all $1 \leq i < n$ and $c_n = 0$. However, this forces p to divide $\deg_{x_i}(M)$ for $2 \leq i < n$ and $\deg_{x_1}(M)$ to be $1 + pc_1$, contradicting Eq. (6.7).

Third, say that M is a monomial of some polynomial in $S^G\, h_{2,a,b}$ for some pair a, b with $1 \leq a \leq b < n$. Eq. (6.7) implies that the degree of x_a or of x_b in each monomial of $h_{2,a,b}$ is too high except the last monomial $N = x_a^{p^{m-1}} x_b^{p^{m-1}} x_n^{2(p-1)p^{m-1}}$. But for any monomial M' appearing in an S^G-multiple of N, p divides $\deg_{x_i}(M')$ for all $i < n$ or $\deg_{x_n}(M') > p^m + e - 1$, contradicting Eq. (6.7) and Eq. (6.6). (One can check the case $p = 2$ separately.) $\square$

Example 6.8. For $G = \left\langle \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \omega \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right) \right\rangle \subset \mathrm{GL}_3(\mathbb{F}_5)$, Proposition 6.5 implies that the space $(S/\mathfrak{m}^{[5^m]})^G$ decomposes as

$$(S^G + \mathfrak{m}^{[5^m]}) \big/ \mathfrak{m}^{[5^m]} \ \oplus \ \mathbb{F}_5[f_1, f_2]\text{-span}\{x_1^{a_1} x_2^{a_2} x_3^{5^m-1} + \mathfrak{m}^{[5^m]} : a_i < 5,\, a_1 + a_2 \geq 2\}\,.$$

In the next result, we do not assume the transvection root space is maximal.

Corollary 6.9. *For any group $G \subset \mathrm{GL}_n(\mathbb{F}_p)$ fixing a hyperplane,*

$$\left({S}/{\mathfrak{m}^{[p^m]}}\right)^G = A_G \oplus B_G\,.$$

Proof. We decompose the vector space V to separate out the trivial action: set

$$V_1 = \mathbb{C}\text{-span}\{v_1, \ldots, v_\ell, v_n\} \quad \text{and} \quad V_2 = \mathbb{C}\text{-span}\{v_{\ell+1}, \ldots, v_{n-1}\}\,,$$

and set $S_1 = S(V_1^*) = \mathbb{F}_p[x_1, \ldots, x_\ell, x_n]$ and $S_2 = S(V_2^*) = \mathbb{F}_p[x_{\ell+1}, \ldots, x_{n-1}]$. Likewise, set $\mathfrak{m}_1^{[p^m]} = (x_1^{p^m}, \ldots, x_\ell^{p^m},\, x_n^{p^m})$ and $\mathfrak{m}_2^{[p^m]} = (x_{\ell+1}^{p^m}, \ldots, x_{n-1}^{p^m})$. Then G is the direct sum $G = G_1 \oplus G_2$ for $G_i = G|_{V_i}$ and $\mathfrak{m}^{[p^m]} = (\mathfrak{m}_1^{[p^m]}, \mathfrak{m}_2^{[p^m]})$. By Proposition 6.5, $(S_1/\mathfrak{m}_1^{[p^m]})^{G_1} = A_{G_1} \oplus B_{G_1}$. Since G_2 acts trivially on V_2, we may set $A_{G_2} = (\mathbb{F}_p[v_{l+1}, \ldots, v_{n-1}] + \mathfrak{m}_2^{[p^m]})/\mathfrak{m}_2^{[p^m]}$ and $B_{G_2} = \{0\}$. The graded isomorphism $S \cong S_1 \otimes_{\mathbb{F}_p} S_2$ induces a graded isomorphism

$$S/\mathfrak{m}^{[p^m]} \quad \cong \quad S_1/\mathfrak{m}_1^{[p^m]} \ \otimes_{\mathbb{F}_p} \ S_2/\mathfrak{m}_2^{[p^m]}$$

and induces graded vector space isomorphisms

$$\left(S/\mathfrak{m}^{[p^m]}\right)^G \cong \left(S_1/\mathfrak{m}_1^{[p^m]}\right)^{G_1} \otimes_{\mathbb{F}_p} \left(S_2/\mathfrak{m}_2^{[p^m]}\right)^{G_2} \cong (A_{G_1} \oplus B_{G_1}) \otimes_{\mathbb{F}_p} A_{G_2} \cong A_G \oplus B_G\,.$$

The result follows since $A_G + B_G \subset (S/\mathfrak{m}^{[p^m]})^G$ (see the proof of Proposition 6.4). □

7. Hilbert Series for maximal transvection root spaces

Again, we assume throughout this section that G is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ fixing a hyperplane H and e is the maximal order of a semisimple element of G. We assume the root space of G is maximal to avoid excessive notation arising from a trivial action of G on extra variables. By Proposition 6.5, $(S/\mathfrak{m}^{[p^m]})^G$ is a direct sum $A_G \oplus B_G$ with invariant subspace A_G described in Sections 4 and 5. For ease with notation, we fix a basis of V as in Section 3 and describe here

$$B_G = \mathbb{F}_p[f_1, \ldots, f_{n-1}]\text{-span}\Big\{x_1^{a_1} \ldots x_{n-1}^{a_{n-1}} x_n^{p^m-1} + \mathfrak{m}^{[p^m]} : 0 \le a_i < p,\, \sum_{i=1}^{n-1} a_i \ge 2\Big\}\,.$$

Lemma 7.1. *Suppose the transvection root space of G is maximal. Then*

$$\mathrm{Hilb}(B_G,\ t) \ = \ t^{p^m-1}\Big(\Big(\frac{1-t^p}{1-t}\Big)^{n-1} - (n-1)t - 1\Big)\Big(\frac{1-t^{p^m}}{1-t^p}\Big)^{n-1}.$$

Proof. Observe that $B_G = \mathbb{F}_p[f_1, \ldots, f_{n-1}]\text{-span}\, C \cong \mathbb{F}_p[f_1, \ldots, f_{n-1}] \otimes_{\mathbb{F}_p} C$ as a graded vector space by Eq. (4.2), where

$$C = \mathbb{F}_p\text{-span}\{x_1^{a_1} \ldots x_{n-1}^{a_{n-1}} x_n^{p^m-1} + \mathfrak{m}^{[p^m]} : 0 \le a_i < p,\, a_1 + \ldots + a_{n-1} \ge 2\}\,.$$

Since $\deg f_i = p$ for $i < n$,

$$\begin{aligned}\mathrm{Hilb}(B_G, t) \ &= \ \Big(\frac{1-t^{p^m}}{1-t^p}\Big)^{n-1} \ \cdot \ \mathrm{Hilb}(C, t)\\ &= \ \Big(\frac{1-t^{p^m}}{1-t^p}\Big)^{n-1} \ t^{p^m-1}\Big(\Big(\frac{1-t^p}{1-t}\Big)^{n-1} - (n-1)t - 1\Big),\end{aligned}$$

with subtracted terms arising from the restriction $a_1 + \ldots + a_{n-1} \geq 2$. □

Theorem 7.2. *Suppose the transvection root space of G is maximal. Then*

$$\mathrm{Hilb}\left(\left(S/\mathfrak{m}^{[p^m]} \right)^G,\ t \right) = \left(\frac{1-t^{p^m}}{1-t^p} \right)^{n-1} \left(\frac{1-t^{p^m-1}}{1-t^e} \right) + t^{p^m-1} \left(\frac{1-t^{p^m}}{1-t} \right)^{n-1}.$$

Proof. By Proposition 6.5, $(S/\mathfrak{m}^{[p^m]})^G = A_G \oplus B_G$, and the theorem follows from adding the Hilbert series for A_G and B_G given in Proposition 5.1 and Lemma 7.1 and simplifying. □

Example 7.3. For our archetype example, $G = \left\langle \left(\begin{smallmatrix} 1&0&0\\0&1&0\\0&0&\omega \end{smallmatrix} \right), \left(\begin{smallmatrix} 1&0&1\\0&1&0\\0&0&1 \end{smallmatrix} \right), \left(\begin{smallmatrix} 1&0&0\\0&1&1\\0&0&1 \end{smallmatrix} \right) \right\rangle \subset \mathrm{GL}_3(\mathbb{F}_5)$, Lemma 7.1 implies that

$$\mathrm{Hilb}(B_G,\, t) = t^{5^m-1} \left(\left(\frac{1-t^5}{1-t} \right)^2 - 2t - 1 \right) \left(\frac{1-t^{5^m}}{1-t^5} \right)^2.$$

By Theorem 7.2 (recall $e = \mathrm{order}(\omega)$), the Hilbert series of $(S/\mathfrak{m}^{[5^m]})^G$ is

$$\left(\frac{1-t^{5^m}}{1-t^5} \right)^2 \left(\frac{1-t^{5^m-1}}{1-t^e} \right) + t^{5^m-1} \left(\frac{1-t^{5^m}}{1-t} \right)^2.$$

We record an alternate expression for the Hilbert series in Theorem 7.2:

Corollary 7.4. *Suppose the transvection root space of G is maximal. Then*

$$\begin{aligned} \mathrm{Hilb}\left(\left(S/\mathfrak{m}^{[p^m]} \right)^G,\ t \right) &= \mathrm{Hilb}(S^G,\, t)(1-t^{p^m})^{n-1} \left(1 - t^{p^m-1} + (1-t^e) t^{p^m-1} \left(\frac{1-t^p}{1-t} \right)^{n-1} \right) \\ &= \left(\frac{1-t^{p^m}}{1-t^p} \right)^{n-1} \left(\left(\frac{1-t^{p^m-1}}{1-t^e} \right) + t^{p^m-1} \left(\frac{1-t^p}{1-t} \right)^{n-1} \right). \end{aligned}$$

8. Hilbert Series for arbitrary group fixing a hyperplane

Again, we assume G is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ fixing a hyperplane H and set $\ell = \dim_{\mathbb{F}_p}(\mathrm{RootSpace}(G)) \cap H$, the dimension of the (not necessarily maximal) transvection root space of G, with e the maximal order of a semisimple element of G.

Theorem 8.1. *Suppose G is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ fixing a hyperplane. Then*

$$\begin{aligned} \mathrm{Hilb}\left(\left(S/\mathfrak{m}^{[p^m]} \right)^G,\ t \right) &= \left(\frac{1-t^{p^m}}{1-t} \right)^{n-\ell-1} \left(\frac{1-t^{p^m}}{1-t^p} \right)^{\ell} \left(\left(\frac{1-t^{p^m-1}}{1-t^e} \right) + t^{p^m-1} \left(\frac{1-t^p}{1-t} \right)^{\ell} \right) \\ &= \left(\frac{1-t^{p^m}}{1-t} \right)^{n-\ell-1} \left(\frac{1-t^{p^m}}{1-t^p} \right)^{\ell} \left(\frac{1-t^{p^m-1}}{1-t^e} \right) + t^{p^m-1} \left(\frac{1-t^{p^m}}{1-t} \right)^{n-1} \\ &= \mathrm{Hilb}(S^G, t)\,(1-t^{p^m})^{n-1} \left((1-t^{p^m-1}) + t^{p^m-1}(1-t^e) \left(\frac{1-t^p}{1-t} \right)^{\ell} \right). \end{aligned}$$

Proof. We write $G = G_1 \oplus G_2$, $S = S_1 \otimes_{\mathbb{F}_p} S_2$, and $\mathfrak{m}^{[p^m]} = (\mathfrak{m}_1^{[p^m]}, \mathfrak{m}_2^{[p^m]})$ as in the proof of Corollary 6.9 and use the graded isomorphism

$$\left(S/\mathfrak{m}^{[p^m]} \right)^G \cong \left(S_1/\mathfrak{m}_1^{[p^m]} \right)^{G_1} \otimes_{\mathbb{F}_p} \left(S_2/\mathfrak{m}_2^{[p^m]} \right)^{G_2}.$$

Since G_2 acts trivially on V_2 of dimension $n - \ell - 1$,

$$\mathrm{Hilb}\left(\left(S/\mathfrak{m}_2^{[p^m]} \right)^{G_2},\ t \right) = \left(\frac{1-t^{p^m}}{1-t} \right)^{n-\ell-1}.$$

Since G_1 has maximal transvection root space in V_1, Corollary 7.4 implies that

$$\mathrm{Hilb}\left(\left(S/\mathfrak{m}_2^{[p^m]}\right)^{G_1},\ t\right) \ = \ \left(\frac{1-t^{p^m}}{1-t}\right)^{n-\ell-1} \left(\frac{1-t^{p^m}}{1-t^p}\right)^{\ell} \left(\left(\frac{1-t^{p^m-1}}{1-t^e}\right) + t^{p^m-1}\left(\frac{1-t^p}{1-t}\right)^{\ell}\right).$$

The theorem then follows from taking the product of the two Hilbert series above. □

Example 8.2. Say $G = \left\langle \begin{pmatrix} 1&0&0\\0&1&0\\0&0&\omega\end{pmatrix}, \begin{pmatrix} 1&0&1\\0&1&0\\0&0&1\end{pmatrix} \right\rangle$, a group without maximal transvection root space, acting on $V = \mathbb{F}_5^3$ with $e = \mathrm{order}(\omega)$. Theorem 8.1 implies

$$\mathrm{Hilb}\left(\left(S/\mathfrak{m}^{[5^m]}\right)^{G},\ t\right) = \left(\frac{1-t^{5^m}}{1-t}\right) \left(\frac{1-t^{5^m}}{1-t^5}\right) \left(\left(\frac{1-t^{5^m-1}}{1-t^e}\right) + t^{5^m-1}\left(\frac{1-t^5}{1-t}\right)\right).$$

We take the limit as t approaches 1 in Theorem 8.1 to obtain the dimension:

Corollary 8.3. *Suppose G is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ fixing a hyperplane. The dimension of $(S/\mathfrak{m}^{[p^m]})^G$ as an $\mathbb{F}_p$-vector space is*

$$\dim_{\mathbb{F}_p}\left(S/\mathfrak{m}^{[p^m]}\right)^{G} = p^{m(n-1)} + p^{m(n-1)-\ell}\left(\frac{p^m-1}{e}\right).$$

Remark 8.4. Note that the Hilbert series in Theorem 8.1 agrees with the series we expect in the nonmodular case, as then all the reflections are semisimple and $\ell = 0$:

$$\mathrm{Hilb}\left(\left(S/\mathfrak{m}^{[p^m]}\right)^{G},\ t\right) \ = \frac{(1-t^{p^m})^{n-1}(1-t^{p^m+e-1})}{(1-t)^{n-1}(1-t^e)}.$$

The basic invariants have degrees $1, \dots, 1, e$ in this case and the series above describes

$$\left(S/\mathfrak{m}^{[p^m]}\right)^{G} \ = \ \mathbb{F}_p[x_1, x_2, \dots, x_{n-1}, x_n^e]/(x_1^{p^m}, \dots, x_n^{p^m}).$$

Compare with [9, Example 1.4].

Remark 8.5. When G contains no semisimple elements (in the modular case), $e = 1$ and ℓ is just the minimum number of generators of G. Theorem 8.1 implies that

$$\mathrm{Hilb}\left(\left(S/\mathfrak{m}^{[p^m]}\right)^{G},\ t\right) = \frac{(1-t^{p^m})^{n-1}(1-t^{p^m-1})}{(1-t^p)^{\ell}(1-t)^{n-\ell}} + t^{p^m-1}\left(\frac{1-t^{p^m}}{1-t}\right)^{n-1}.$$

9. Full Pointwise Stabilizers over $\mathbb{F}_q$ and Orbits

The story is more complicated when generalizing to arbitrary finite fields $\mathbb{F}_q$ for q a prime power. The basic invariants for an arbitrary subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ fixing a hyperplane H in $V = \mathbb{F}_q^n$ pointwise can be described inductively (see [7]). However, some of the previous ideas apply to give the Hilbert series for full pointwise stabilizer subgroups. Throughout this section, fix a hyperplane H in $V = \mathbb{F}_q^n$ and consider the pointwise stabilizer group $G = \mathrm{GL}_n(\mathbb{F}_q)_H = \{g \in \mathrm{GL}_n(\mathbb{F}_q) : g|_H = 1\}$. In this case, S^G is again a polynomial ring: After change-of-basis, we may assume $S^G = \mathbb{F}_q[\tilde{f}_1, \dots \tilde{f}_n]$ for

$$\tilde{f}_1 = x_1^q - x_1 x_n^{q-1}, \dots, \tilde{f}_{n-1} = x_{n-1}^q - x_{n-1}x_n^{q-1}, \quad \tilde{f}_n = x_n^{q-1}.$$

Many results from our previous sections hold for these full stabilizer subgroups; for brevity, we highlight below only the more subtle changes in the arguments.

Define polynomials in $\mathbb{F}_q[\tilde{f}_1, \ldots, \tilde{f}_n]$ for $1 \leq a \leq b < n$ by

$$\tilde{h}_0 = \tilde{f}_n^{\,1+(q-1)^{-1}(q^m-1)},\ \tilde{h}_{1,a} = \sum_{k=0}^{m-1} \tilde{f}_n^{\,1+(q-1)^{-1}(q^m-q^{m-k})}\, \tilde{f}_a^{\,q^{m-k-1}},\ \tilde{h}_{2,a,b} = \tilde{f}_a^{\,q^{m-1}}\, \tilde{f}_b^{\,q^{m-1}}.$$

The next observation is an analog of Lemma 4.5; the proof is straight-forward.

Lemma 9.1. *For $G = \mathrm{GL}_n(\mathbb{F}_q)_H$, $\tilde{h}_0$, $\tilde{h}_{1,a}$, $\tilde{h}_{2,a,b}$ lie in $S^G \cap \mathfrak{m}^{[q^m]}$ for $1 \leq a \leq b < n$.*

The next result, analogous to Lemma 4.6, uses a monomial ordering as in Section 4.

Lemma 9.2. *Say $G = \mathrm{GL}_n(\mathbb{F}_q)_H$ and f in $S^G \cap \mathfrak{m}^{[q^m]}$ is homogeneous in the variables $\tilde{f}_1, \ldots, \tilde{f}_n$. Then $\mathrm{LM}_{S^G}(f)$ is divisible by $\tilde{f}_n$ or some $\tilde{h}_{2,a,b}$ with $1 \leq a \leq b < n$.*

Proof. The argument follows the proof of Lemma 4.6 with p changed to q and e to $q-1$ until Eq. (4.7), which, in our setting, becomes

$$d = q^{m-1} + (q-1)a \quad \text{and} \quad i = 1 + qa \quad \text{for some} \quad 0 \leq a < \sum_{k=0}^{m-2} q^k\,. \tag{9.3}$$

We use the base p expansions of a and d to show instead that $\sum_{k=0}^{m-2} q^k \leq a$, writing

$$a = \sum_{k=0}^{(m-2)r} a_k\, p^k \quad \text{and} \quad d = \sum_{k=0}^{(m-1)r} d_k\, p^k \quad \text{for some} \quad 0 \leq a_k,\, d_k < p\,.$$

We compare the base p coefficients d_k and a_k. Lucas' Theorem implies that

$$0 \neq \binom{d}{i} = \binom{d_0}{1} \prod_{k=1}^{r-1} \binom{d_k}{0} \prod_{k=r}^{(m-1)r} \binom{d_k}{a_{k-r}} \quad \text{as } i = 1 + \sum_{k=r}^{(m-1)r} a_{k-r}\, p^k\,;$$

since no factor in the product vanishes, we conclude that $d_0 \geq 1$ and each $a_{k-r} \leq d_k$ for $r \leq k \leq (m-1)r$. Eq. (9.3) then provides direct comparison of d_k and a_k,

$$\sum_{k=0}^{(m-1)r} d_k\, p^k \;=\; d \;=\; q^{m-1} - \sum_{k=0}^{r-1} a_k p^k + \sum_{k=r}^{(m-2)r} (a_{k-r} - a_k) p^k + \sum_{k=(m-2)r}^{(m-1)r} a_{k-r} p^k. \tag{9.4}$$

We now regroup base p as needed and show inductively that $0 < a_0 \leq a_r \leq \ldots \leq a_{(m-2)r}$. More generally, we will show $a_k \leq a_{k+r}$ for $0 \leq k \leq (m-3)r$ when $m > 2$.

First consider a_0. Since $1 \leq d_0$, Eq. (9.4) implies that $d_0 = p - a_0$ and $a_0 \neq 0$. Thus $d_i = p - a_i - 1$ for $1 \leq i \leq r-1$ since $d_i \geq 0$. For $m > 2$, next observe that $a_0 \leq a_r$ since $a_0 \leq d_r$ and Eq. (9.4) implies that $d_r = p + a_0 - a_r - 1$ for $a_0 \leq a_r$ whereas $d_r = a_0 - a_r - 1$ for $a_r < a_0$. Similarly, $a_1 \leq a_{r+1}$ since $a_1 \leq d_{r+1}$ and Eq. (9.4) implies that $d_{r+1} = p + a_1 - a_{r+1} - 1$ for $a_1 \leq a_{r+1}$ whereas $d_{r+1} = a_1 - a_{r+1} - 1$ for $a_{r+1} < a_1$. We iterate this argument and conclude that $a_k \leq a_{k+r}$ for $0 \leq k \leq (m-3)r$. In particular, $0 < a_0 \leq a_r \leq \ldots \leq a_{r(m-2)}$. The result follows as in the proof of Lemma 4.6. $\square$

We adapt the proofs of Propositions 4.9 and 5.1 using Lemmas 9.1 and 9.2 to obtain

Proposition 9.5. *For $G = \mathrm{GL}_n(\mathbb{F}_q)_H$,*

- *$\{\tilde{h}_0,\, \tilde{h}_{1,a},\, \tilde{h}_{2,a,b} : 1 \leq a \leq b < n\}$ is a Groebner basis of $S^G \cap \mathfrak{m}^{[q^m]}$,*

- $\mathrm{Hilb}\left(S^G + \mathfrak{m}^{[q^m]} \big/ \mathfrak{m}^{[q^m]},\ t\right) = \left(\frac{1-t^{q^m}}{1-t^q}\right)^{n-1} \left(\frac{1-t^{q^m+q-2}+(n-1)\,t^{q^m}(1-t^{q-1})}{1-t^{q-1}}\right).$

The next result is an analog of Lemma 6.2; we have only found case-by-case arguments for generalizing this key lemma to arbitrary subgroups G fixing a single hyperplane.

Lemma 9.6. *Say $G = \mathrm{GL}_n(\mathbb{F}_q)_H$. Suppose $f + \mathfrak{m}^{[q^m]}$ lies in $(S/\mathfrak{m}^{[q^m]})^G$ with f homogeneous in $x_1, \ldots, x_n$. Then $\mathrm{LM}_S(f)$ lies in*

$$\mathfrak{m}^{[q^m]} \qquad or \quad \mathbb{F}_q[x_1, \ldots, x_{n-1}, \tilde{f}_n^{(q^m-1)/(q-1)}] \quad or \quad \mathbb{F}_q[x_1^q, \ldots, x_{n-1}^q, \tilde{f}_n]\,.$$

Proof. Say $M = \mathrm{LM}_S(f)$ does not lie in $\mathfrak{m}^{[q^m]}$ or in $\mathbb{F}_q[x_1, \ldots, x_{n-1}, \tilde{f}_n^{(q^m-1)/(q-1)}]$. Then

$$M = x_1^{b_1} \cdots x_k^{b_k} \cdots x_{n-1}^{b_{n-1}}\, x_n^{b_n} \qquad \text{for some } \ b_1, \ldots, b_{n-1} < q^m \text{ and } b_n < q^m - 1\,.$$

Invariance under the generator g_n of the semisimple elements in G implies that b_n is divisible by $q-1$ as in the proof of Lemma 6.2 and so $b_n \leq q^m - q$.

Say q does not divide some b_k with $k < n$. Let g in $\mathrm{GL}_n(\mathbb{F}_q)_H$ be the element mapping x_k to $x_k + x_n$ and fixing x_i for $i \neq k$ as in Section 4. Arguments as in the proof of Lemma 6.2 show that p divides b_k and thus

$$b_k = p^t c_k \quad \text{ for } t < r = \dim_{\mathbb{F}_p}(\mathbb{F}_q) \text{ and } \gcd(p, c_k) = 1.$$

We argue that the monomial $x_\beta = M \cdot (x_n/x_k)^{p^t}$ lies outside $\mathfrak{m}^{[q^m]}$ but appears with nonzero coefficient in $gf - f$, contradicting the fact that $gf - f \in \mathfrak{m}^{[q^m]}$. The leading term of $gM - M$ in $\mathbb{F}_q[x_1, \ldots, x_n]$ is $c_k x_\beta \neq 0$ as $\binom{p^t c_k}{p^t} = \binom{c_k}{1}$ by Lucas' Theorem. We claim that for any other monomial N of f, the coefficient of x_β in $gN - N$ is zero. Since g fixes x_i with $i \neq k$, we may assume $\deg_{x_i}(N) = \deg_{x_i}(M)$ for $i \neq k$, $i < n$. Since $\mathrm{LM}_S(f) = M$, $\deg_{x_k}(N) < b_k$ and $\deg_{x_n}(N) > b_n$. But $q-1$ divides $\deg_{x_n}(N)$ as f is invariant under the diagonal reflection sending x_n to x_n^{q-1} and thus $\deg_{x_n}(N) \geq b_n + q - 1$ and $\deg_{x_k}(gN - N) \leq \deg_{x_k}(N) \leq b_k - q + 1 < b_k - p^t = \deg_{x_k} x_\beta$, and the coefficient of x_β in $gN - N$ is zero. Note that $gf - f \notin \mathfrak{m}^{[q^m]}$ since $b_n + p^t < q^m$ as $b_n \leq q^m - q$. $\square$

We obtain a direct sum decomposition analogous to Proposition 6.5.

Proposition 9.7. *For $G = \mathrm{GL}_n(\mathbb{F}_q)_H$, the invariants are $\left(S \big/ \mathfrak{m}^{[q^m]}\right)^G = A_G \oplus B_G$ for*

$$A_G = (S^G + \mathfrak{m}^{[q^m]})/\mathfrak{m}^{[q^m]} \qquad \textit{and}$$

$$B_G = \mathbb{F}_q[\tilde{f}_1, \ldots, \tilde{f}_{n-1}]\text{-}\textit{span}\Big\{x_1^{a_1} \ldots x_{n-1}^{a_{n-1}} x_n^{q^m-1} + \mathfrak{m}^{[q^m]},\ \textit{for } 0 \leq a_i < q, \sum_{i=1}^{n-1} a_i \geq 2\Big\}.$$

Proof. One may easily adapt the proofs of Proposition 6.4 and Proposition 6.5 to the case of $\mathbb{F}_q$ using Proposition 9.5 and Lemma 9.6. $\square$

The proof of Lemma 7.1 can be modified to give the Hilbert series of B_G:

Lemma 9.8. *For any hyperplane H in $V = \mathbb{F}_q^n$ and $G = \mathrm{GL}_n(\mathbb{F}_q)_H$,*

$$\mathrm{Hilb}(B_G,\ t) \ = \ t^{q^m-1}\Big(\Big(\frac{1-t^q}{1-t}\Big)^{n-1} - (n-1)t - 1\Big)\Big(\frac{1-t^{q^m}}{1-t^q}\Big)^{n-1}.$$

Finally, Propositions 9.5 and 9.7 and Lemma 9.8 give Theorem 1.1 of the Introduction:

Corollary 9.9. *For any hyperplane H in $V=\mathbb{F}_q^n$ and $G=\mathrm{GL}_n(\mathbb{F}_q)_H$,*

$$\begin{aligned}\mathrm{Hilb}\left(\left({S}\big/{\mathfrak{m}^{[q^m]}}\right)^G,\ t\right) &= \left(\frac{1-t^{q^m}}{1-t^q}\right)^{n-1}\left(\left(\frac{1-t^{q^m-1}}{1-t^{q-1}}\right)+t^{q^m-1}\left(\frac{1-t^q}{1-t}\right)^{n-1}\right)\\ &= \mathrm{Hilb}(S^G,\,t)(1-t^{q^m})^{n-1}\left(1-t^{q^m-1}+(1-t^{q-1})t^{q^m-1}\left(\frac{1-t^q}{1-t}\right)^{n-1}\right)\\ &= [q^{m-1}]_{t^q}^{n-1}\begin{bmatrix}m\\1\end{bmatrix}_{q,t}+t^{q^m-1}[q^m]_t^{n-1}\begin{bmatrix}m\\0\end{bmatrix}_{q,t}.\end{aligned}$$

We take the limit $t\mapsto 1$ for the following corollary.

Corollary 9.10. *For any hyperplane H in $V=\mathbb{F}_q^n$ and $G=\mathrm{GL}_n(\mathbb{F}_q)_H$,*

$$\dim_{\mathbb{F}_q}\left({S}\big/{\mathfrak{m}^{[q^m]}}\right)^G = q^{m(n-1)}+q^{(m-1)(n-1)}\left(\frac{q^m-1}{q-1}\right).$$

Orbits and the dimension of the invariant space. The conjecture of Lewis, Reiner, and Stanton [9] giving the Hilbert series for the $\mathrm{GL}_n(\mathbb{F}_q)$-invariants in $S/\mathfrak{m}^{[q^m]}$ specializes to a conjecture for the dimension of the invariants as an $\mathbb{F}_q$-vector space. They show this specialization gives the number of orbits for $\mathrm{GL}_n(\mathbb{F}_q)$ acting on the vector space $V'=(\mathbb{F}_{q^m})^n$, see [9, Section 7.1 and Theorem 6.16].

Corollary 8.3 gives the dimension of the G-invariants in $S/\mathfrak{m}^{[p^m]}$ over $\mathbb{F}_p$ for any group G fixing a hyperplane. Below we prove that this integer gives the number of orbits for G as a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ acting on the vector space $V'=(\mathbb{F}_{p^m})^n$ (with canonical coordinate-wise action induced from the embedding $\mathbb{F}_p\subset\mathbb{F}_{p^m}$). This result thus proves a special case of the conjecture of Lewis, Staton, and Reiner. Here again, $\ell=\dim_{\mathbb{F}_p}(\mathrm{RootSpace}(G))\cap H$ with e the maximal order of a semisimple element in G.

Corollary 9.11. *Suppose $G\le\mathrm{GL}_n(\mathbb{F}_p)$ is a reflection group fixing a hyperplane H in $V=\mathbb{F}_p^n$. The number of orbits of points in $V'=(\mathbb{F}_{p^m})^n$ under the action of G is equal to the dimension over $\mathbb{F}_p$ of the G-invariants in $S/\mathfrak{m}^{[p^m]}$:*

$$\dim_{\mathbb{F}_p}\left({S}\big/{\mathfrak{m}^{[p^m]}}\right)^G \ =\ p^{m(n-1)}+p^{m(n-1)-\ell}\left(\frac{p^m-1}{e}\right)\ =\ \#\text{ orbits of } G \text{ on } (\mathbb{F}_{p^m})^n\,.$$

Proof. Corollary 8.3 records the dimension; we count orbits here. Let H' be the image of H under the coordinate-wise embedding $V\hookrightarrow V'$. Choose a basis $x_1,\dots,x_n$ of $(V')^*$ dual to the standard coordinate basis as in Section 3 with $H'=\operatorname{Ker}x_n$ in V'. The number of points with orbit size 1 is the number of points on the hyperplane H', namely, $(p^m)^{n-1}$. Two points v and u lying in the complement $(H')^c$ of H' in V' lie in the same G-orbit if and only if $x_i(v)=x_i(u)$ for $i\le\ell$ and $x_n(u)$ lies in $\mathbb{F}_px_1(v)+\cdots+\mathbb{F}_px_\ell(v)+\langle\omega\rangle x_n(v)$ for ω a primitive e-th root-of-unity in $\mathbb{F}_p$. Thus a fixed v in $(H')^c$ has orbit size $p^\ell e$ whereas $|(H')^c|=(p^m)^{n-1}(p^m-1)$ and

$$\#\text{ of orbits in }(H')^c=\frac{|(H')^c|}{\text{size of an orbit in }(H')^c}=p^{m(n-1)-\ell}\left(\frac{p^m-1}{e}\right).$$

The total number of orbits for $\mathrm{GL}_n(\mathbb{F}_p)_H$ acting on $\mathbb{F}_{p^m}$ is then

$$\begin{aligned}\#\text{ of orbits}\ &=\ (\#\text{ orbits on }H')+(\#\text{ orbits on }(H')^c)\\ &=\ p^{m(n-1)}+p^{m(n-1)-\ell}\left(\frac{p^m-1}{e}\right).\end{aligned}$$

□

A similar proof with q for p and $q-1$ for e using Corollary 9.10 gives Corollary 1.2 from the Introduction; we suspect a similar statement holds for any reflection group:

Corollary 9.12. *For any hyperplane H in $V = \mathbb{F}_q^n$, the number of orbits in $(\mathbb{F}_{q^m})^n$ under the action of $G = \mathrm{GL}_n(\mathbb{F}_q)_H$ is*

$$\dim_{\mathbb{F}_q} \left({}^{S}\!/\!_{\mathfrak{m}^{[q^m]}} \right)^G = q^{m(n-1)} + q^{(m-1)(n-1)} \left(\frac{q^m-1}{q-1} \right) = q^{m(n-1)} \begin{bmatrix} m \\ 0 \end{bmatrix}_q + q^{(m-1)(n-1)} \begin{bmatrix} m \\ 1 \end{bmatrix}_q .$$

10. Lewis, Reiner, and Stanton conjecture

We use our results in previous sections to bound the exponents of $x_1, \ldots, x_n$ in any invariant of $S/\mathfrak{m}^{[q^m]}$ under the full general linear group $\mathrm{GL}_n(\mathbb{F}_q)$ for a prime power q.

Proposition 10.1. *Say $f + \mathfrak{m}^{[q^m]} \in (S/\mathfrak{m}^{[q^m]})^{\mathrm{GL}_n(\mathbb{F}_q)}$. For any monomial $M \notin \mathfrak{m}^{[q^m]}$ in $x_1, \ldots, x_n$ of f, either $M = x_1^{q^m-1} x_2^{q^m-1} \cdots x_n^{q^m-1}$ or $\deg_{x_i}(M) \le q^m - q$ for all i.*

Proof. We may assume f is homogeneous in $x_1, \ldots, x_n$ with no monomials lying in $\mathfrak{m}^{[q^m]}$. By Lemma 9.6 with hyperplane $H = \operatorname{Ker} x_n$ and ordering $x_1 > \cdots > x_n$,

$$\mathrm{LM}(f) \in \mathbb{F}_q[x_1, \ldots, x_{n-1}, x_n^{q^m-1}] \quad \text{or} \quad \mathrm{LM}(f) \in \mathbb{F}_q[x_1^q, \ldots, x_{n-1}^q, x_n^{q-1}] .$$

First suppose $\deg_{x_n}(\mathrm{LM}(f)) = q^m - 1$. The element $f + \mathfrak{m}^{[q^m]}$, and hence f itself, is invariant under the action of the symmetric group $\mathfrak{S}_n$ permuting the variables as a subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$. This forces $\mathrm{LM}(f) = x_1^{q^m-1} \cdots x_n^{q^m-1} = f$, as f is homogeneous.

Now assume $\deg_{x_n}(\mathrm{LM}(f)) \ne q^m - 1$, so that q divides $\deg_{x_1}(\mathrm{LM}(f))$. Since f is invariant under the diagonal reflection with $x_1 \mapsto \omega x_1$ for ω a primitive $(q-1)$-th root-of-unity, $(q-1)$ also divides $\deg_{x_1}(\mathrm{LM}(f))$. Therefore, $q(q-1)$ divides $\deg_{x_1}(\mathrm{LM}(f))$ and $\deg_{x_1}(\mathrm{LM}(f)) \le q^m - q$. Then $\deg_{x_1}(M) \le q^m - q$ for any monomial M of f. As f is $\mathfrak{S}_n$-invariant, $\deg_{x_i}(M) \le q^m - q$ for all i as well. $\square$

The previous proposition gives a bound on coefficients of the Hilbert series. Let HF be the *Hilbert function*, $\mathrm{HF}(M, i) = \dim_{\mathbb{F}} M_i$, for any $\mathbb{Z}$-graded vector space $M = \bigoplus M_i$.

Corollary 10.2. *We give a bound on the Hilbert function of $\mathrm{GL}_n(\mathbb{F}_q)$-invariants:*

$$\mathrm{HF}\Big(\big({}^{S}\!/\!_{\mathfrak{m}^{[q^m]}} \big)^{\mathrm{GL}_n(\mathbb{F}_q)}, n(q^m-1) \Big) = 1 \quad \textit{and}$$
$$\mathrm{HF}\Big(\big({}^{S}\!/\!_{\mathfrak{m}^{[q^m]}} \big)^{\mathrm{GL}_n(\mathbb{F}_q)}, i \Big) \le \mathrm{HF}\Big({}^{S}\!/\!_{(x_1^{q^m-q+1}, \ldots, x_n^{q^m-q+1})}, i \Big) \quad \textit{for } i \ne n(q^m-1) .$$

11. Two dimensional vector spaces

We now consider the 2-dimensional case and take a group G of $\mathrm{GL}_2(\mathbb{F}_p)$ fixing a hyperplane (line) of $V = (\mathbb{F}_p)^2$ pointwise. Here, $\mathfrak{m}^{[p^m]} := (x_1^{p^m}, x_2^{p^m})$. We give a resolution of $S^G \cap \mathfrak{m}^{[p^m]}$ directly using syzygies, providing an alternate direct computation for the Hilbert series of $A_G = (S^G + \mathfrak{m}^{[p^m]})/\mathfrak{m}^{[p^m]}$.

Nonmodular Setting. If G contains no transvections, then $S^G \cap \mathfrak{m}^{[p^m]}$ is generated by $h = f_1^{p^m}$ and $h' = f_2^{1+e^{-1}(p^m-1)}$ and we obtain an easy resolution for $S^G \cap \mathfrak{m}^{[p^m]}$,

$$0 \longrightarrow F_1 \xrightarrow{[\tau]} F_0 \xrightarrow{[h\ h']} S^G \cap \mathfrak{m}^{[p^m]} \longrightarrow 0\,,$$

where $F_1 = S^G[-(2p^m + e - 1)]$ and $F_0 = S^G[-p^m] \oplus S^G[-(p^m + e - 1)]$ with relation $\tau = f_2^{1+e^{-1}(p^m-1)} h - f_1^{p^m} h'$. This gives Hilbert series

$$\mathrm{Hilb}(S^G \cap \mathfrak{m}^{[p^m]},\ t) = \frac{t^{p^m} + t^{p^m+e-1} - t^{2p^m+e-1}}{(1-t^e)(1-t)} = \mathrm{Hilb}(S^G,\ t)(t^{p^m} + t^{p^m+e-1} - t^{2p^m+e-1})\ .$$

Modular setting. Suppose now that G contains a transvection. After conjugation, $G = \langle \left(\begin{smallmatrix} 1 & 0 \\ 0 & \omega \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle$ for some root-of-unity $\omega \in \mathbb{F}_p$ of order $e \geq 1$. Here,

$$S^G = \mathbb{F}_p[x_1, x_2]^G = \mathbb{F}_p[f_1, f_2] \quad \text{ for } f_1 = x_1^p - x_1 x_2^{p-1} \text{ and } f_2 = x_2^e\,.$$

The Groebner basis

$$h_0 = f_2^{1+e^{-1}(p^m-1)}, \quad h_1 = \sum_{k=0}^{m-1} f_2^{1+e^{-1}(p^m - p^{m-k})}\, f_1^{p^{m-k-1}}, \quad h_2 = f_1^{2p^{m-1}}$$

(see Definition 4.3) of the ideal $S^G \cap \mathfrak{m}^{[p^m]}$ in the polynomial ring S^G is small enough to directly provide a manageable resolution of $S^G / S^G \cap \mathfrak{m}^{[p^m]}$, which we record below.

Proposition 11.1. *For G a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ containing a transvection, a graded free resolution of the S^G-module $S^G \cap \mathfrak{m}^{[p^m]}$ is*

$$0 \longrightarrow F_1 \xrightarrow{[\tau_{0,1}\ \ \tau_{1,2}]} F_0 \xrightarrow{[h_0\ h_1\ h_2]} S^G \cap \mathfrak{m}^{[p^m]} \longrightarrow 0$$

for

$$\begin{aligned} F_0 &= S^G\big[-(p^m+e-1)\big] \oplus S^G\big[-(p^m+e)\big] \oplus S^G[-2p^m], \qquad \textit{and} \\ F_1 &= S^G\big[-(2p^m+e)\big] \oplus S^G\big[-(2p^m+e-1)\big]\,. \end{aligned}$$

Proof. Buchberger's algorithm gives generators for the first syzygy-module in $(S^G)^3$ for $S^G \cap \mathfrak{m}^{[p^m]} = (h_0, h_1, h_2)$, namely,

$$\tau_{0,1} = (-f_1^{p^{m-1}} - \sum_{k=1}^{m-1} f_1^{p^{m-k-1}}\, f_2^{e^{-1}(p^m-p^k)},\ f_2^{e^{-1}(p^m-1)},\ 0)$$

$$\tau_{0,2} = (f_1^{2p^{m-1}},\ 0,\ -f_2^{1+e^{-1}(p^m-1)}), \qquad \text{and}$$

$$\tau_{1,2} = (-\sum_{j,k=1}^{m-1} f_1^{p^{m-j-1}+p^{m-k-1}}\, f_2^{e^{-1}(p^m-p^k-p^j+1)},\ -f_1^{p^{m-1}} + \sum_{k=1}^{m-1} f_1^{p^{m-k-1}}\, f_2^{e^{-1}(p^m-p^k)},\ f_2)\,.$$

But $\tau_{0,2}$ is redundant as

$$\tau_{0,2} = \Big(\sum_{k=1}^{m-1} f_1^{p^{m-k-1}}\, f_2^{e^{-1}(p^m-p^k)} \tau_{0,1} - f_1^{p^{m-1}}\Big)\tau_{0,1} - f_2^{e^{-1}(p^m-p^k)} \tau_{1,2}\,,$$

and the first syzygy-module is generated over S^G by just $\tau_{1,2}$ and $\tau_{0,1}$. As these are linearly independent over S^G, the second syzygy-module is trivial, and the result follows. $\square$

This gives an easy proof of Proposition 5.1 in the modular 2-dimensional setting:

Corollary 11.2. *For G a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ fixing a hyperplane in $V = (\mathbb{F}_p)^2$ and containing a transvection,*

$$\mathrm{Hilb}\left({(S^G + \mathfrak{m}^{[p^m]})}\big/{\mathfrak{m}^{[p^m]}},\ t \right) = \mathrm{Hilb}(S^G,\ t)(1 - t^{p^m})(1 + t^{p^m} - t^{p^m+e-1} - t^{p^m+e})\,.$$

Proof. By Proposition 11.1, the Hilbert series for $S^G \cap \mathfrak{m}^{[p^m]}$ is just the series for F_1 subtracted from that for F_0. The proposition then follows from using the exact sequence

$$0 \longrightarrow S^G \cap \mathfrak{m}^{[p^m]} \longrightarrow S^G \longrightarrow {S^G}\big/{(S^G \cap \mathfrak{m}^{[p^m]})} \cong {(S^G + \mathfrak{m}^{[p^m]})}\big/{\mathfrak{m}^{[p^m]}} \longrightarrow 0.$$

$\square$

References

[1] D. Armstrong, V. Reiner, B. Rhoades, *Parking spaces*, Adv. Math., 269 (2015), 647–706.

[2] Y. Berest, P. Etingof, and V. Ginzburg, *Finite-dimensional representations of rational Cherednik algebras*, Int. Math. Res. Not. 19 (2003), 1053–1088.

[3] D. Bessis and V. Reiner, *Cyclic sieving of noncrossing partitions for complex reflection groups*, Ann. Comb. 15 (2011), no. 2, 197–222.

[4] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics, 150, Springer-Verlag, New York, 1995, xvi+785.

[5] I. Gordon, *On the quotient ring by diagonal invariants*, Invent. Math., 153 (2003), 503–518.

[6] I. Gordon and S. Griffeth, *Catalan numbers for complex reflection groups*, Amer. J. Math. 134 (2012), no. 6, 1491–1502.

[7] J. Hartmann and A.V. Shepler, *Jacobians of reflection groups*, Trans. Amer. Math. Soc, 360 (2008), 123–133.

[8] C. Krattenthaler, T. Müller, *Cyclic sieving for generalised non-crossing partitions associated with complex reflection groups of exceptional type.* In *Advances in combinatorics*, 209–247, Springer, Heidelberg, 2013.

[9] J. Lewis, V. Reiner and D. Stanton, *Invariants of $GL_n(F_q)$ in polynomials mod Frobenius powers*, Proc. Roy. Soc. Edinburgh Sect. A, 147 (2017), 831–873.

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

[11] V. Reiner and D. Stanton, *(q,t)-analogues and $GL_n(\mathbb{F}_q)$*, J. Algebraic Combin. 31 (2010), 411–454.

[12] R. P. Stanley, *Enumerative combinatorics. Vol. 1*, Cambridge Studies in Advanced Mathematics, 49, With a forward by G. Rota, Corrected reprint of the 1986 original, Cambridge University Press, 1997, xii+325.

[13] C. Stump, *q,t-Fuß-Catalan numbers for finite reflection groups*, J. Algebr. Comb. (2010) 32, 67–97.

Department of Mathematics, University of North Texas, Denton, Texas 76203, USA
Email address: chelseadrescher@my.unt.edu

Department of Mathematics, University of North Texas, Denton, Texas 76203, USA
Email address: ashepler@unt.edu